funkwerk
enterprise communications

User Manual

funkwerk W500

Copyright © February 2010 Funkwerk Enterprise Communications GmbH
Version 2.1

Purpose

This document describes the installation and usage of the **funkwerk W500.**

Liability

While every effort has been made to ensure the accuracy of all information in this manual, Funkwerk Enterprise Communications GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information and changes can be found at www.funkwerk-ec.com.

Trademarks

Product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

Copyright

All rights are reserved. No part of this publication may be reproduced or transmitted in any form or by any means – graphic, electronic, or mechanical – including photocopying, recording in any medium, taping, or storage in information retrieval systems, without the prior written permission of Funkwerk Enterprise Communications GmbH. Adaptation and especially translation of the document is inadmissible without the prior consent of Funkwerk Enterprise Communications GmbH.

Guidelines and Standards

Funkwerk products comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

You will find detailed information in the Declarations of Conformity at www.funkwerk-ec.com.

How to Reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH
Suedwestpark 94
D-90449 Nuremberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

1 Introduction 7
1.1 Technical Features and Advantages 7
1.2 System Configurations 8
2 Hardware Installation 9
2.1 Checking for Completeness 9
2.2 System Requirements 9
2.3 Mechanical Description 10
2.4 Hardware Installation 12
3 Configuration 15
3.1 Access to the Web-based Configuration Program 15
3.1.1 Status 17
3.1.2 System 18
3.2 Wireless 19
3.2.1 WPS Settings 19
3.2.2 Wireless Settings 20
3.2.3 Security 28
3.2.4 MAC Address Filter 38
3.3 Management 40
3.3.1 Password 40
3.3.2 Configuration File 41
3.3.3 Upgrade Firmware 42
3.4 Monitoring 43
3.4.1 Logs 43
3.4.2 Statistics 44
3.4.3 List of Associated Devices 45

4 Use of the Device in Various Network Scenarios 47

4.1 Bridge Mode with WEP 47
4.1.1 Login 47
4.1.2 Navigation Menu 48
4.1.3 Setting Operation Mode 49
4.1.4 Advanced Settings / Setting MAC Address 50
4.1.5 Checking Status 52

4.2 Access Point Mode with WPA2-PSK and MAC Filter 53
4.2.1 Login 54
4.2.2 Navigation Menu 55
4.2.3 Setting Operation Mode 56
4.2.4 Setting the Security Mode 58
4.2.5 Checking Status 61

4.3 AP + Repeater Mode with WPA2-PSK 62
4.3.1 Login 63
4.3.2 Navigation Menu 64
4.3.3 Setting Operation Mode 65
4.3.4 Setting the Security Mode 67

4.4 Wireless Client Mode with WPA2-PSK 67
4.4.1 Login 68
4.4.2 Navigation Menu 68
4.4.3 Setting Operation Mode 69
4.4.4 Wireless Client 71
4.4.5 Security Mode for the Wireless Client 74
4.4.6 Checking the Client's Status 75

5 Warranty 77

5.1 Replacement, Repair and Refund for Hardware 78

5.2 Technical Data 80

6 Safety Precautions 81

6.1 General Safety Precautions in English 82

6.2 Allgemeine Sicherheitshinweise in Deutsch 85

6.3 Indicaciones generales de seguridad en español 89

6.4 Consignes générales de sécurité en français 93

6.5 Indicazioni generali di sicurezza in italiano 96

6.6 Ogólne instrukcje bezpieczeñstwa w jêzyku polskim 99

6.7 Considerações genéricas em matéria de segurança, em português 103

1 Introduction

This product was specially designed to satisfy the needs of small offices or home offices.

It represents a complete solution for wireless networking and is very easy to configure and operate without any special prior technical knowledge. This Manual contains instructions for installing and configuring **W500**. Please read this Manual thoroughly before you install and use this product. This way you will be able to derive the maximum benefit from the functionality of the device.

1.1 Technical Features and Advantages

- Interoperable with IEEE 802.11g wireless devices
- Support for AP, wireless client, repeater and bridge modes
- High security: WEP encryption (64, 128 and 152 bit), 802.1x (EAP-TLS, EAP-TTLS, LEAP, EAP-PEAP), WPA/WPA-PSK, WPA2/WPA2-PSK, wireless MAC filter list
- Direct interface to IEEE 802.3 Fast Ethernet networks (10/100-BaseTX RJ-45 LAN port)
- Supports data rates of 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- Wi-Fi Protected Setup (WPS) allows users to automatically establish a connection between **W500** and WPS-capable wireless clients. Users can configure the wireless client for the connection with **W500** at the press of a button.

1.2 System Configurations

W500 can be set up for a wealth of network systems configurations.

Wireless Infrastructure

In a wireless infrastructure, **W500** acts as an access point (AP) with repeater. The access point links wireless clients with one another. Here the AP is at the center of all wireless communication. This makes communication more efficient, because the wireless adapters do not have to be within direct range of each other.

Wireless Infrastructure with Stations in the Wired LAN

W500 allows access to your wired LAN. A LAN with integrated wired and wireless components is known as infrastructure configuration. A group of WLAN-PC users and an access point form a basic service set (BSS). Each wireless connected PC in this BSS can make contact with every computer in your wired network via the access point.

2 Hardware Installation

This chapter describes the initial setup of the access point (AP).

2.1 Checking for Completeness

Make sure the following parts are present prior to installation:

- W500
- Ethernet cable
- Power supply unit
- Product CD

If any of these parts are missing or damaged, please contact your vendor for further assistance.

2.2 System Requirements

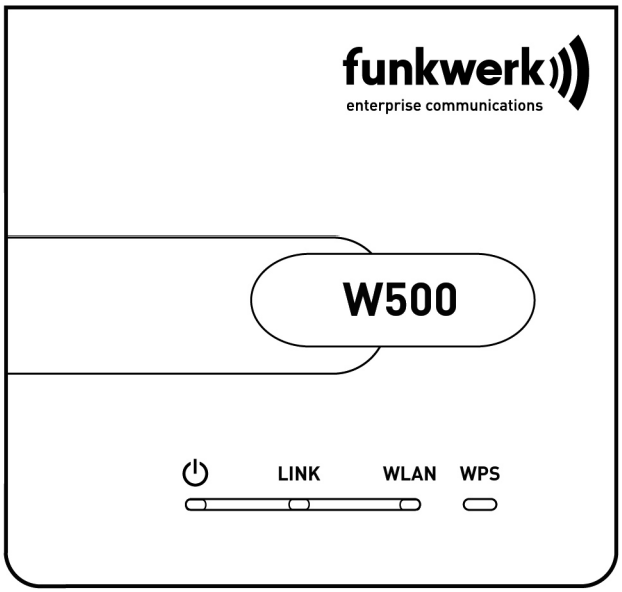
Required for installing **W500**:

1. A power socket (100~240 V, 50~60 Hz) for power supply to the access point.

2. An Ethernet network.

2.3 Mechanical Description

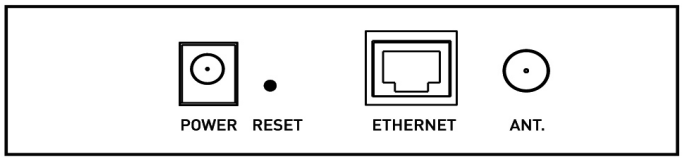
Top side of **W500**:



The following table describes the LEDs and their significance:

LED designation	Color	Description
	Steady green	Power supply established.
LINK	Orange	***ON:*** 10 Mbps connection established at LAN port.
		BLINKING: Sending or receiving data via the LAN port.
	Green	***ON:*** 100 Mbps connection established at LAN port.
		BLINKING: Sending or receiving data via the LAN port.
WLAN	Green	***BLINKING:***Sending or receiving data via the wireless connection.
WPS button/LED	-----	After activating WPS in "Push Button" mode, to be used as described in Chapter 4.2.1.

W500 rear panel:



Connection/ operating element	Description
POWER	Power supply: 12 V DC, 1.0 A (min.).
RESET	The Reset button resets the system settings to the factory defaults. Keep the Reset button depressed for at least three seconds. After releasing the button **W500** reboots.
ETHERNET	LAN port 10/100 Mbps Ethernet
ANT	The antenna is included with the device. Please screw the antenna into the jack (ANT) and align it vertically.

2.4 Hardware Installation

Perform the following steps to set up **W500**.

Select Location

Decide on the location of **W500** before installation. The location must be carefully selected in order to ensure the best radio range for **W500**. The most favorable location for installing **W500** is usually at the center of the required radio coverage area. Attempt to install the mobile stations within line of sight of **W500**. Obstacles can impair the performance of **W500**.

Positioning W500

You can place **W500** on a flat surface such as a table or cupboard or mount the unit upright e.g. on a wall. The **W500** antenna works best in an open environment with as few obstacles as possible.

Connecting the Ethernet Cable

W500 supports a 10/100 Mbps Ethernet connection. Connect one end of the Ethernet cable to the **W500** RJ-45 connector. Connect the other end of the RK-45 cable with a switch, hub or computer.

Establishing Power Supply

Connect the power supply unit with the power supply. **W500** automatically starts a self-test. Wait for around a minute until the WLAN LED is lit steady and **W500** switches to normal operation.

Note

The W500 access point must only be operated with the approved power supply unit supplied.

Defining Settings for Wireless Devices

For accessing **W500** the wireless devices (802.11b or 802.11g standard) must be configured according to the **W500** settings. The default settings for **W500** are as follows:

NETWORK NAME: *Funkwerk-ec*

CHANNEL: *6*

OPERATING MODE: *AP*

WLAN SECURITY: *OFF*

Note

It is strongly recommended to set ***WLAN SECURITY*** to *ON* and to change the **W500** security mode from*disabled (default settings)* to *WPA2-PSK* (recommended setting). Please find the necessary setup steps in Chapter 4.2.4 (Setting Security Mode).

3 Configuration

W500 allows IP configuration via the ComPoint Manager and detailed set-up with a web browser.

3.1 Access to the Web-based Configuration Program

If you do not wish to use the fixed **W500** IP address*192.168.0.252*, please install the ComPoint Manager software. You can find it on the product CD or on our website. ComPoint Manager allows you to localize **W500** within your network without difficulty and define another IP address suitable for the network. The use of ComPoint Manager is explained in the documentation for this tool.

Note

Not all functions of FEC ComPoint Manager are available for **W500**. The localization of devices in the network and the IP configuration of FEC devices are supported. Please note that **W500** is not compatible with the Funkwerk WLAN management software applications WILMA or WMS.

The following instructions guide you through the installation of **W500** with the example of its preset IP address.

1. Connect your computer wireless or via a cable to **W500**. Please set a fixed IP address on your computer. It must be in the range *192.168.0.X*, whereby "*X*" must not be *254* or *252*. If you wish to establish a wireless connection, you first have to set the configuration described below in the computer.
   - ***SSID:*** *Funkwerk-ec*
   - ***CHANNEL:*** *6*
   - ***WLAN SECURITY****: disabled*
   - ***OPERATION MODE:*** *AP*
   - ***WLAN:*** *ON*
2. Open your web browser, in the address field enter the **W500** IP address and press Enter. The **W500** standard address is http://192.168.0.252.

3. The ***USER*** is *'admin'* and the default ***PASSWORD*** is *'funkwerk'.*

The web-based configuration program offers you several options for monitoring and configuring **W500**.

After logging on you arrive at the homepage. Here you find the buttons **Status, System, Wireless LAN, Management** and **Monitoring**. The main menu contains links to all parts of the web configuration interface.

3.1.1 Status

The ***STATUS*** page offers a brief description of the device and its status. The displayed device status includes ***DEVICE INFORMATION, IP SETTINGS*** and ***WIRELESS SETTINGS***.

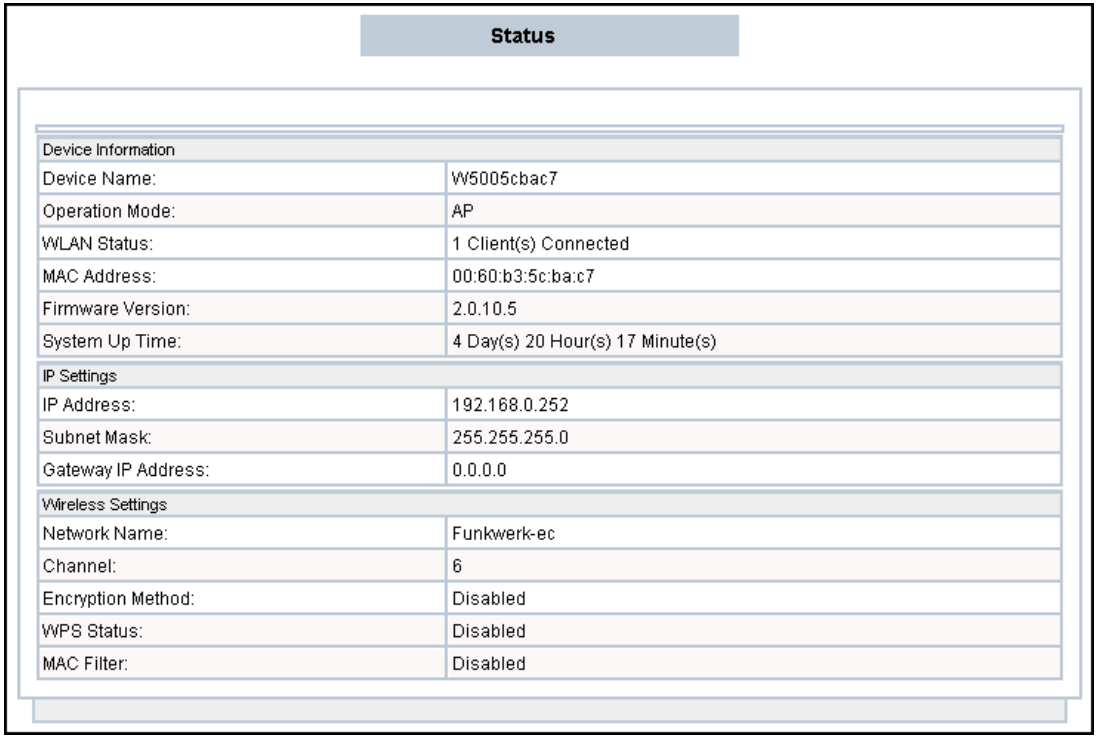


Figure 3-1: Status

3.1.2 System

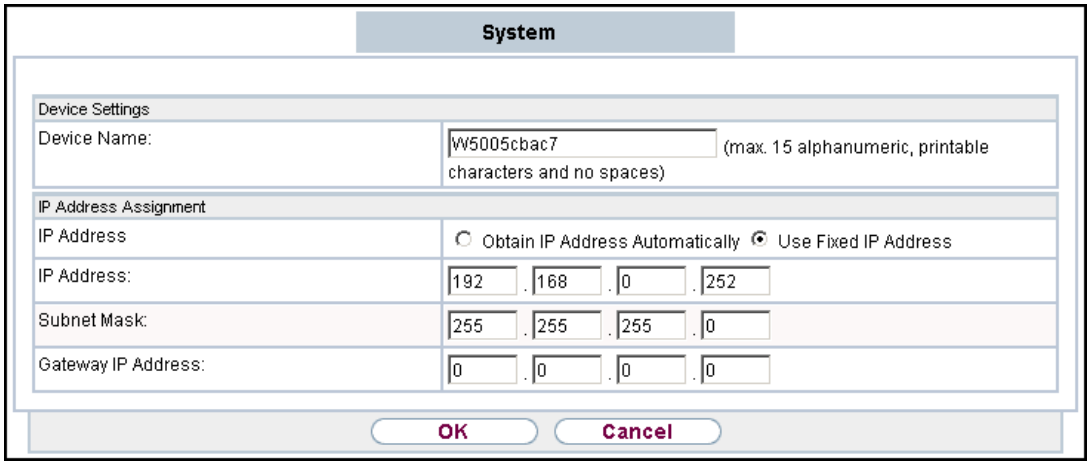


Figure 3-2: System

DEVICE SETTINGS: The device name serves to identify your access point. The default is **W500** plus the 6 last digits of the MAC address.

This makes it easier for you to manage your access point if there are several APs in your network. You can also use the name of the AP for web management access (e.g. http://W5005cbac7).

IP ADDRESS ASSIGNMENT: You can define the IP address for your access point in this section. You have the option of using a fixed IP address or of obtaining the IP address automatically using DHCP.

Note

On completion of the settings, click **OK** to implement the changes.

3.2 Wireless

3.2.1 WPS Settings

The WPS (Wi-Fi Protected Setup) specification is overseen by the Wi-Fi Alliance and primarily serves to simplify setup and management of security functions for Wi-Fi networks.

The access point supports three WPS configuration methods: **Client's PIN, AP's PIN** and **Push Button**. To enable the WPS function click the check box ***ENABLE WPS***.

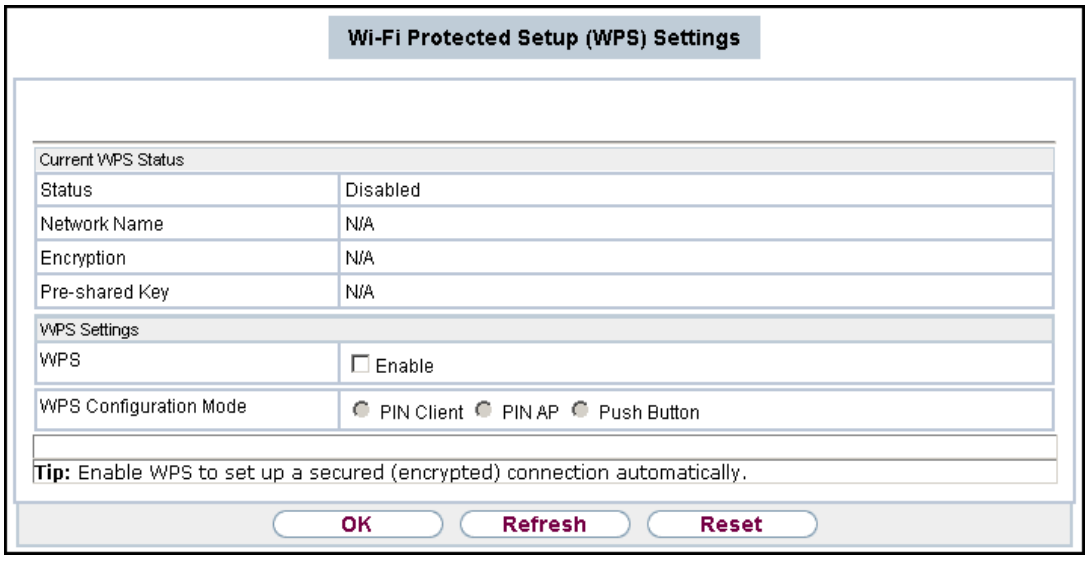


Figure 3-3: WPS settings

PIN Client After selecting the WPS configuration method **PIN Client** enter the PIN and the pre-shared key generated from the WPS wireless client on attempting to establish connection with the AP. Alternatively, you can enter your own PSK. Click **OK** to immediately start the WPS process.

PIN AP If the **PIN AP** WPS configuration method is selected, the AP automatically generates a PIN. Click **OK** to save the configuration and to enter the generated PIN in the wireless client WPS program. In this case, start the process start from the wireless client WPS program.

Push Button **W500** supports software PBC (calling up WPS mode from a software button) and hardware PBC (calling up WPS mode by pressing a button on the device). To use software PBC, select **WPS Configuration Mode Push Button** and enter the pre-shared key. Click **Start PBC** to start the WPS process. If you wish to use the hardware WPS button, the **WPS Enable** check box must be selected. Keep the Hardware WPS button depressed for at least three seconds. After releasing the button the AP switches to the WPS mode for two minutes. During these two minutes you have to arrange for the wireless client to establish a WPS connection with the AP using the same PBC mode.

3.2.2 Wireless Settings

In this menu you can undertake changes to the settings for wireless network operation. In ***General Settings*** changes can be made to ***Operation Mode***, ***Network Name***, ***Channel*** and ***Wireless Mode,*** in ***Advanced Settings*** additional parameters such as ***Output power*** or ***Data Rate Management*** are accessible for changing.

Figure 3-4: Wireless settings

Fields in the General Settings menu

Field	Description
OPERATION MODE	Define in which mode the wireless module of your device is to be operated Selectable parameters: – *Access point:* Your device serves as an access point in your network. – *Bridge*: Your device serves as a wireless bridge in your network. The device can act as a wireless network bridge and establish wireless connections to other APs. In this case, you have to know the MAC address of the other peer devices, which must also be in bridge mode. If two APs are connected in bridge mode, they form a WDS (Wireless Distribution System), which allows computers in a LAN to establish contact with the computers in another LAN. – *AP+Repeater*: Select *AP+Repeater* as operation mode if the device is to work as an access point and wireless bridge. – *Wireless Client*: In this mode the device behaves like a wireless client connected with a wireless network.

Field	Description
NETWORK NAME (SSID):	The ***NETWORK NAME (SSID)*** is an identification used by access points and stations, which is unique for a WLAN. The standard SSID is *funkwerk-ec*. To change this, please enter the required name of the wireless network. The SSID must consist of a maximum of 32 ASCII characters. Also select whether the ***NETWORK NAME (SSID)*** is to be transferred. The function becomes enabled with the selection of *Visible*. This is set to enabled by default.
CHANNEL:	Select the channel from the list box, which is appropriate for your network settings.
WIRELESS MODE:	Select the wireless technology, which the access point is to use. Selectable values: – ***AUTO***: default value. Your device adapts to the technology (802.11b or 802.11g) of the clients. – ***ONLY 802.11b:*** Your device works exclusively to 802.11b and the clients must adapt accordingly. – ***ONLY 802.11g:*** Your device works exclusively to 802.11g and the clients must adapt accordingly. 802.11b clients do not have access.

Fields in the WDS Settings menu

Field	Description
LOCAL MAC ADDRESS:	The MAC address of the device.
REMOTE MAC ADDRESS 1-4:	Enter the MAC address of the peer device in a format valid for MAC addresses (six hexadecimal character pairs).

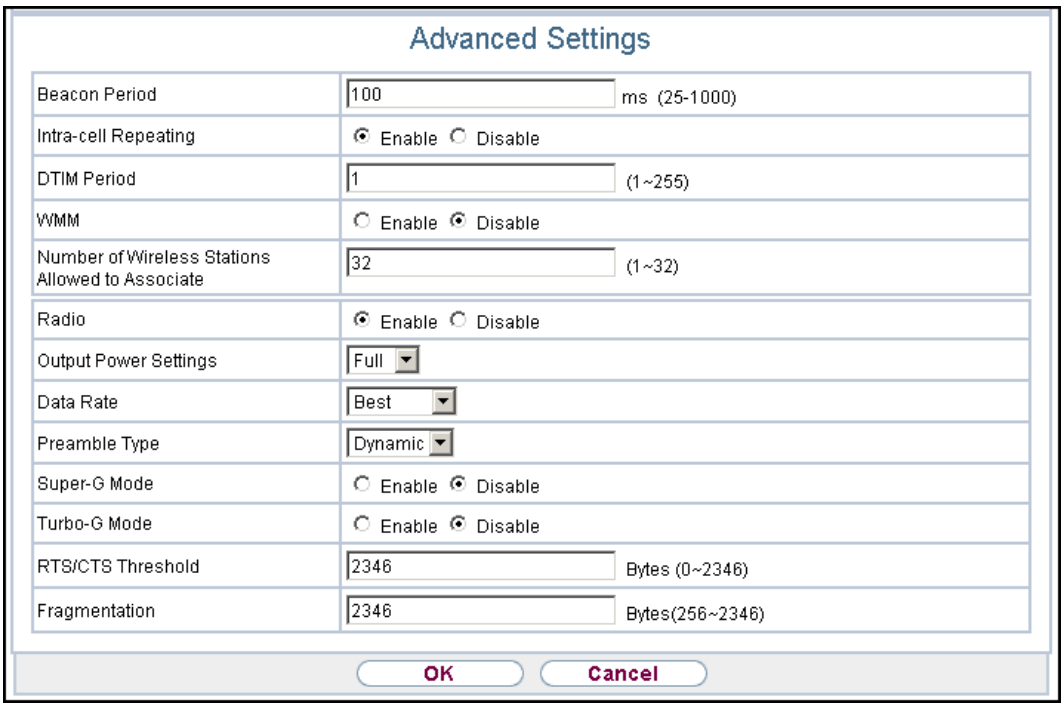


Figure 3-5: Advanced settings

Fields in the Advanced Settings menu

Field	Description
BEACON PERIOD:	Enter the time in milliseconds between sending two beacons. This value is transferred to Beacon and Probe Response Frames. The default value is *100* msec.
INTRA-CELL REPEATING:	Select whether communication between the WLAN clients within a wireless cell is to be allowed The function becomes enabled with the selection of *Enabled*. By default, the function is *Enabled*.
DTIM PERIOD:	Specify the interval for the Delivery Traffic Indication Message (DTIM). The DTIM field is a data field in the transmitted beacons, which informs clients about the next broadcast or multicast transmission. If the clients are operated in the power-saving mode, they will wake up in time and will receive the data. Values are possible between *1* and *255* The default value is *1*.

Field	Description
WMM:	Select whether WMM (Wireless Multimedia) is to be enabled for wireless network voice or video data prioritization, in order to always attain the best possible transmission quality for time-critical applications. DSCP (Differentiated Services Code Point) or IEEE802.1d data prioretization is supported. The function becomes enabled with the selection of *Enabled*.
NUMBER OF CLIENTS ALLOWED TO BE LOGGED ON AT THE SAME TIME:	Use this field to define the maximum number of wireless stations that can have a connection with the device. Enter the number (*1* to *32*) of permissible wireless stations.
RADIO:	Enable the wireless adapter to allow wireless communication between the device and other devices in accordance with IEEE802.11b or IEEE802.11g standards. Disable the wireless adapter to terminate wireless communication between the device and other devices in accordance with IEEE802.11b or IEEE802.11g standards.
OUTPUT POWER:	Defines the output power of the access point. The options are *Full, 50%, 25%, 12%, Min*. The default setting (*50%*) is matched to the 5dBi antenna supplied. The output power must not be increased when using the 5dBi antenna.

Field	Description
DATA RATE MANAGEMENT	The underlying transmission rate should be selected dependent on the speed of the wireless network. The value determines this transmission rate. From the drop-down menu select *Best*, to always achieve the highest possible transmission rate.
PREAMBLE TYPE:	The preamble defines the length of the PLCP synchronization field for communication between the access point ad the network interface card. The default setting is *Dynamic*.
SUPER-G MODE:	Enabling the Super-G mode can improve the wireless data throughput. The default setting is *Disabled*.
TURBO-G MODE:	Enabling Turbo-G can improve the wireless data throughput up to 108 Mbps. Please note that to use this mode the wireless client also has to support the Turbo-G mode. The default setting is *Disabled*. ***NOTE***: Only certain WLAN devices and WLAN clients support this mode.
RTS/CTS THRESHOLD:	The RTS Threshold serves to prevent the occurrence of hidden node problems. RTS is activated if the size of the packet sent is larger than a defined value. If RTS is activated, the station and your access point use a RTS/CTS method for data transmission. The setting range extends from 0 to 2346.

Field	Description
FRAGMENTATION:	Specify the maximum size above which the data packages are fragmented (i.e. divided into smaller units). Low values in this field are recommended in areas with poor reception and interference. Values are possible between *256* and *2346* The default value is *2346* bytes.

Note

On completion of the settings, click **OK** to implement the changes.

3.2.3 Security

As WLAN data are sent via the transmission medium of open space, data can, in theory, be intercepted and read by anybody with the appropriate means. For this reason, the protection of the wireless link deserves special attention.

Access control

By creating an access control list (ACL mode or MAC filter), you can control which clients are allowed to access your wireless LAN. In the access control list, specify the MAC addresses of the clients which are allowed to access to your wireless LAN. Access is denied to all other clients.

802.1x authentication

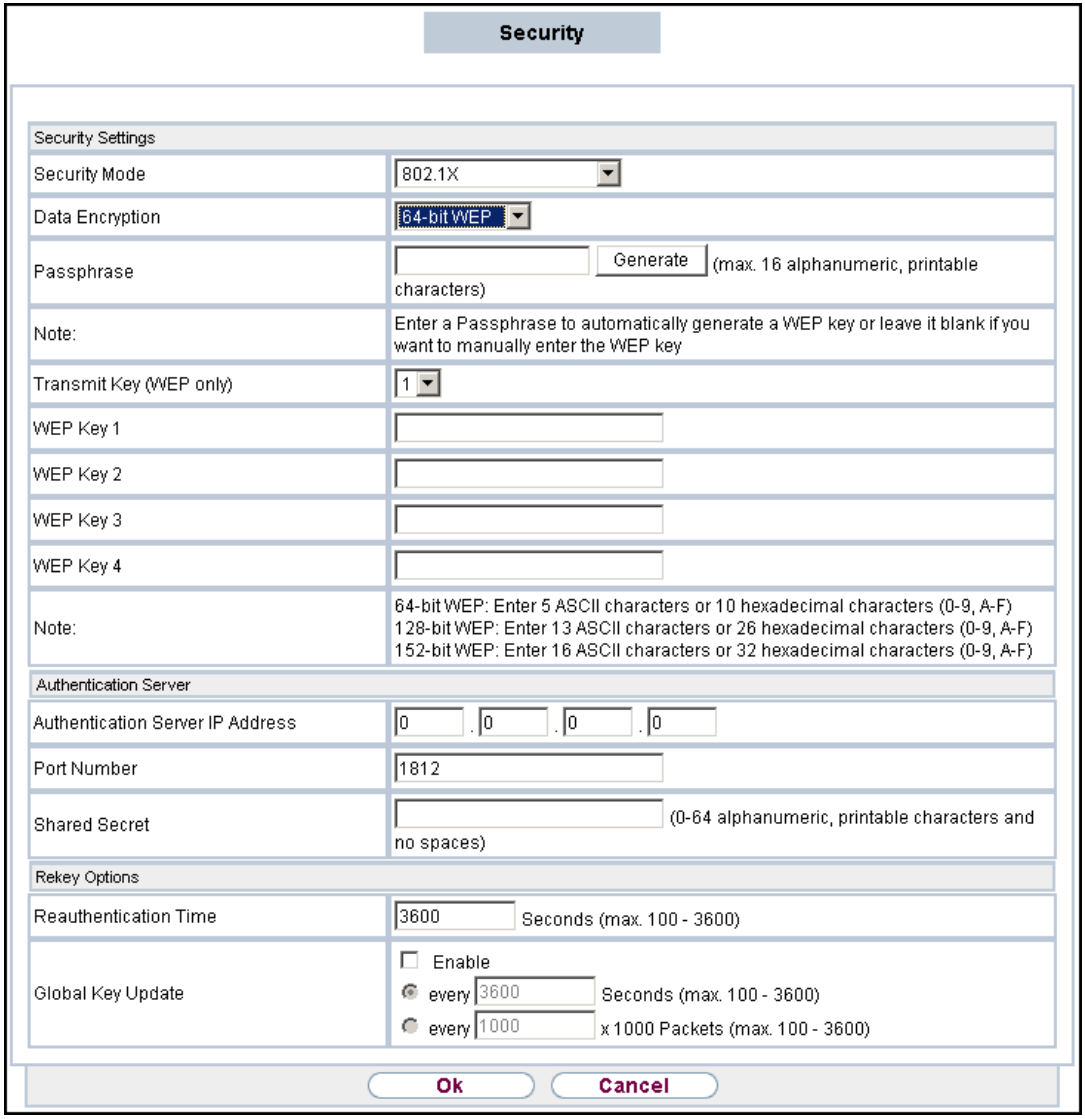

Security
Security Settings
Security Mode
802.1X
Data Encryption
64-bit WEP
Passphrase
Generate
(max. 16 alphanumeric, printable characters)
Note:
Enter a Passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key
Transmit Key (WEP only)
1
WEP Key 1
WEP Key 2
WEP Key 3
WEP Key 4
Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)
152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters (0-9, A-F)
Authentication Server
Authentication Server IP Address
0 . 0 . 0 . 0
Port Number
1812
Shared Secret
(0-64 alphanumeric, printable characters and no spaces)
Rekey Options
Reauthentication Time
3600
Seconds (max. 100 - 3600)
Global Key Update
Enable
every 3600 Seconds (max. 100 - 3600)
every 1000 x 1000 Packets (max. 100 - 3600)
Ok
Cancel

Figure 3-6: 802.1x security

Field	Description
SECURITY MODE:	**802.1x authentication:** **IEEE 802.1x** is a standard for network access control (port-based), specially introduced for distributing cryptographic keys in a wireless network. The access point supports IEEE 802.1x to repel non-authorized users and to check the authorization of users with RADIUS so that authorized users obtain access to the network and services. To use **IEEE 802.1x** you require a common Extensible Authentication Protocol (EAP) on your authorization server, the APs (authenticator) and the stations (requestor). **IEEE 802.1x** is also used to generate and distribute cryptographic keys from the AP to the station as part of the authentication process. Another factor here is the dynamic **WEP**. It is based on old RC4 WEP encryption and with this access point is available under the setting to enable **IEEE 802.1x** security in association with disabled *Wired Equivalent Privacy (WEP)* settings. Key lengths are selectable as 64 or 128 bit. The longer the key, the greater the security it offers.
DATA ENCRYPTION:	After clicking the button **Set WEP Key** you can define the *Length, Format, Key Index* and *Passphrase* for the WEP key.

Field	Description
PASSPHASE:	You can also input the ***PASSPHRASE*** manually: ***64-BIT WEP:*** Enter five ASCII characters or 10 hexadecimal values (between 0-9, a-f and A-F). ***128-BIT WEP:***Enter 13 ASCII characters or hexadecimal values (between 0-9, a-f and A-F). ***152-BIT WEP:*** Enter 16 ASCII characters or 32 hexadecimal values (between 0-9, a-f and A-F).
TRANSMISSION KEY (WEP ONLY):	Select one of the keys configured in **WEP Key <1-4>** as the standard key. The default value is *Key 1*.
AUTHENTICATION SERVER IP ADDRESS:	Enter the IP address of the RADIUS server.
PORT NUMBER:	Enter the associated port for RADIUS data. According to RFC 2138, the standard ports reserved are 1812 for authentication (1645 in older RFCs) and 1813 for billing (1646 in older RFCs). You can find out which port is to be used from the documentation on your RADIUS server. The default value is *1812*.
SHARED SECRET:	Enter your shared password for communication between the RADIUS server and your device.
REAUTHENTICATION TIME:	Here you can enter the time interval within which the connection is reauthenticated. The default value is *3600*.
GLOBAL KEY UPDATE	Here you can define whether the key to protect the connection is renewed at regular intervals. You can select between renewal after a certain period of time or on receipt and/or transmission of a certain number of packets. The default status of this function is disabled.

WEP

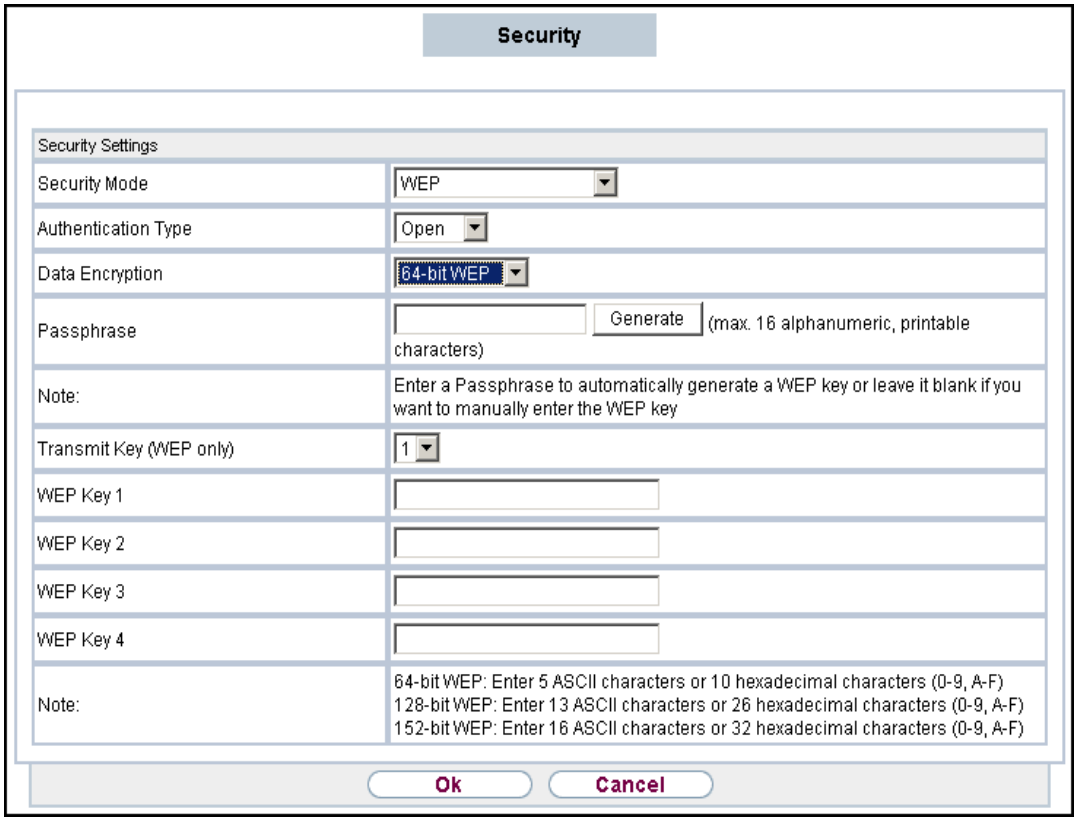

Security
Security Settings
Security Mode
WEP
Authentication Type
Open
Data Encryption
64-bit WEP
Passphrase
Generate
(max. 16 alphanumeric, printable characters)
Note:
Enter a Passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key
Transmit Key (WEP only)
1
WEP Key 1
WEP Key 2
WEP Key 3
WEP Key 4
Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)
152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters (0-9, A-F)
Ok
Cancel

Figure 3-7: Security WEP

Field	Description
SECURITY MODE:	***WEP:*** 802.11 defines the WEP (Wired Equivalent Privacy) security standard. The widely use WEP standard has been shown to be susceptible. Hence, the WPA or WPA2 pre-shared key should preferably be used.
AUTHENTICATION TYPE:	***OPEN:*** Requires no authentication, as it allows the participation of all the devices in the network without a previous security check. The authentication method is set to *Open* in the pre-settings. ***SHARED KEY:*** The station and access point must use the same WEP key for authentication.. In simple terms, WEP must be enabled and configured for the **access point** and **client** and the same key used. All points in the network must use the same authentication method.
DATA ENCRYPTION:	After clicking the button **Set WEP Key** you can define the *Length, Format, Key Index* and *Passphrase* for the WEP key.
PASSPHASE:	You can also input the ***PASSPHRASE*** manually: ***64-BIT WEP:*** Enter five ASCII characters or 10 hexadecimal values (between 0-9, a-f and A-F). ***128-BIT WEP:***Enter 13 ASCII characters or hexadecimal values (between 0-9, a-f and A-F). ***152-BIT WEP:*** Enter 16 ASCII characters or 32 hexadecimal values (between 0-9, a-f and A-F).
TRANSMISSION KEY (WEP ONLY):	Select one of the keys configured in **WEP Key <1-4>** as the standard key. The default value is *Key 1*.

Note

The WEP passphrase must be exactly the same for wireless clients and **W500**. If you define *0011223344* for **W500**, you also have to assign all other client stations the WEP passphrase *0011223344*.

WPA & WPA2

W500 offers WPA and WPA2 setting options for even higher security in wireless network operation. Wi-Fi Protected Access (WPA) is part of the IEEE 802.11i standard. WPA2 is a wireless security standard, which, compared with WPA, offers more effective encryption, authentication and key management.

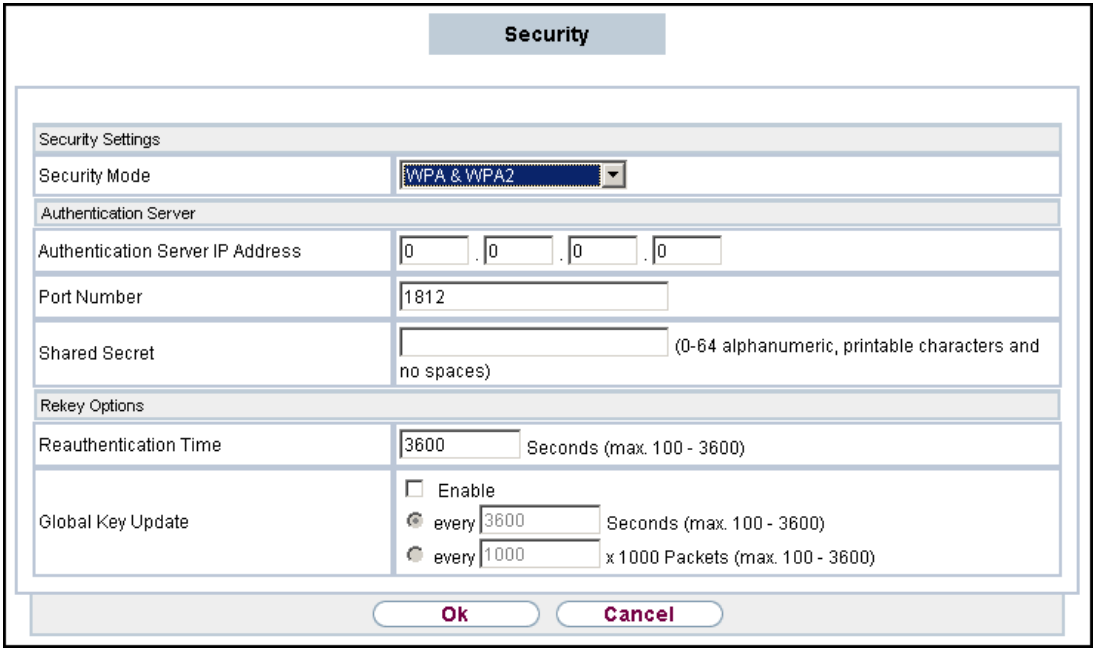


Figure 3-8: WPA & WPA2 security

Field	Description
SECURITY MODE:	**WPA** WPA (Wi-Fi Protected Access) offers additional protection with dynamic keys, based on the Temporal Key Integrity Protocol (TKIP) and offering authentication of users' PSK (Pre Shared Keys) or the Extensible Authentication Protocol (EAP) with 802.1x (e.g. RADIUS). Authentication via EAP is generally used in large wireless LAN installations, as this requires an authentication service in the form of a server (e.g. a RADIUS server). PSKs are generally used in smaller networks, as often occur in SoHo (Small Office, Home Office) environments. The corresponding PSK must therefore be known to all subscribers in the wireless LAN, because it is used to generate the session key. **WPA2** The advancement on WPA is WPA2. Not only has the 802.11i standard been fully implemented in WPA2, but it also uses another encryption algorithm (AES, Advanced Encryption Standard).
AUTHENTICATION SERVER IP ADDRESS:	Enter the IP address of the RADIUS server.

Field	Description
PORT NUMBER:	Enter the associated port for RADIUS data. According to RFC 2138, the standard ports reserved are 1812 for authentication (1645 in older RFCs) and 1813 for billing (1646 in older RFCs). You can find out which port is to be used from the documentation on your RADIUS server. The default value is *1812*.
SHARED SECRET:	Enter your shared password for communication between the RADIUS server and your device.
REAUTHENTICATION TIME:	Here you can enter the time interval within which the connection is reauthenticated. The default value is *3600*.
GLOBAL KEY UPDATE	Here you can define whether the key to protect the connection is renewed at regular intervals. You can select between renewal after a certain period of time or on receipt and/or transmission of a certain number of packets. The default status of this function is disabled.

WPA Authentication Mode: **W500** offers two selection options: **Enterprise (RADIUS)** and **Personal (Pre-Shared Key)**. After selecting **Enterprise** you have to enter the RADIUS server data, otherwise you have to enter the pre-shared key format and the pass-phrase.

WPA Cipher Suite: Using WPA as the encryption method, the WPA Cipher presetting is *TKIP* only.

WPA2 Cipher Suite: Using WPA2 as the encryption method, the WPA Cipher presetting is *AES* only.

WPA-PSK & WPA2-PSK

Note

The security modes are available both in pure form, as well as in mixed form.

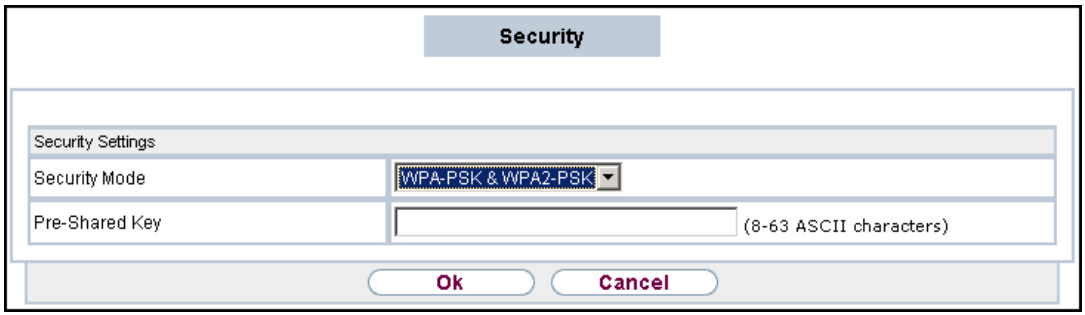


Figure 3-9: WPA-PSK & WPA2-PSK security

Note

Windows XP as a client operating system requires at least SP2 and update KB 893357 for WPA2.

3.2.4 MAC Address Filter

The MAC address filter allows the configuration of the AP such that the access point only allows certain wireless stations exclusive access or selected stations are denied this access. To enable the WPS filter function, click the check box beside **Enable**. Select **Allow the following MAC Address to associate** and enter the MAC address of the wireless client in order to allow the specified wireless stations access to the wireless network. Alternatively, select **Deny the following MAC Address to associate** in order to deny the specified wireless stations access to the wireless network.

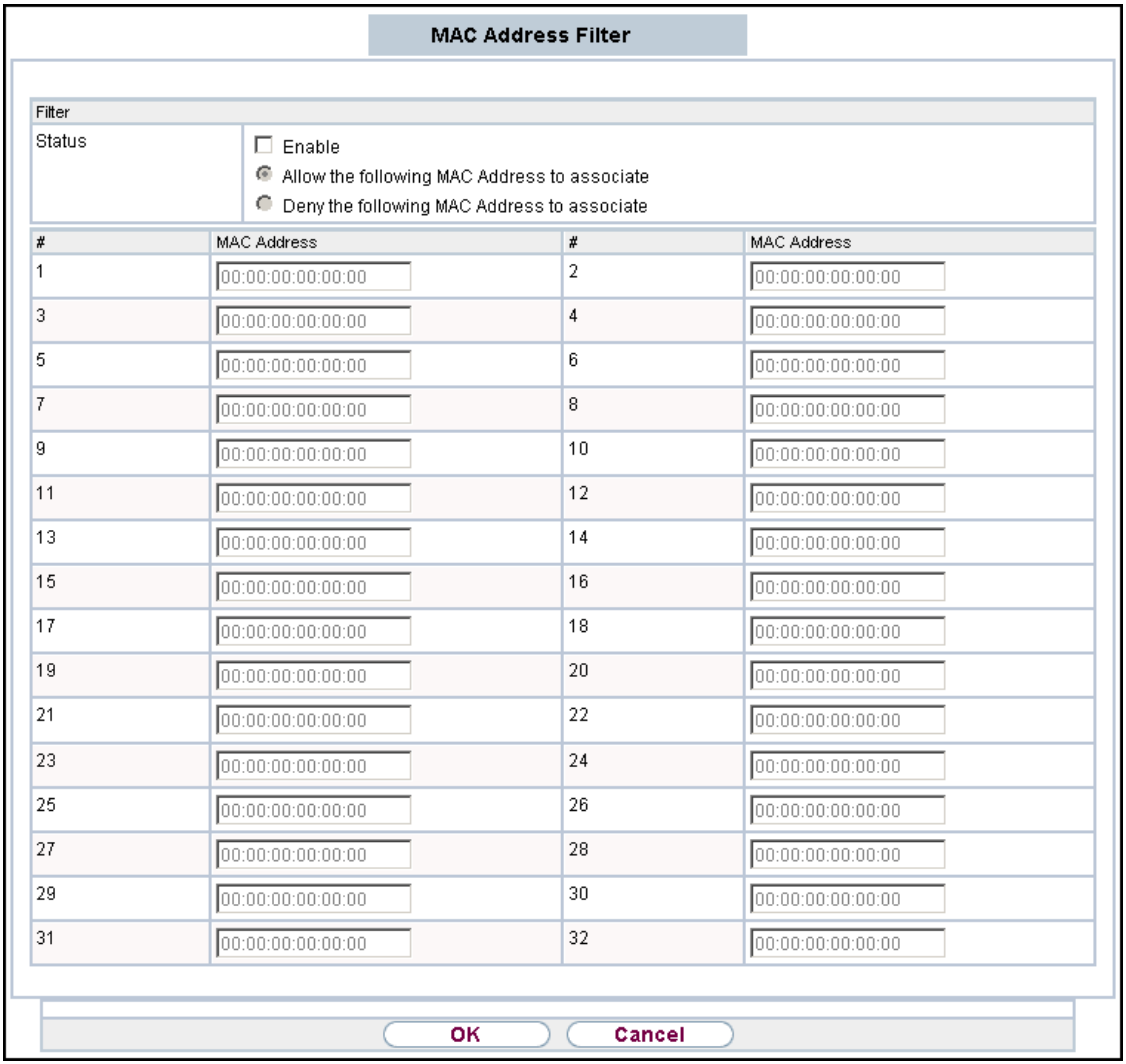


Figure 3-10: MAC Address Filter

3.3 Management

3.3.1 Password

Here you can change the password for the access point as explained below.

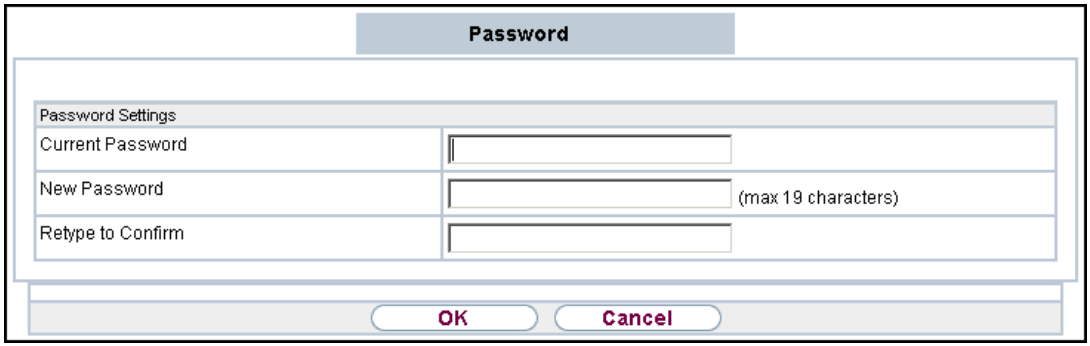


Figure 3-11: Password

1. To change the current password, select in the **Management** section the option **Password** on the left hand side.
2. Enter the new password for **W500** into the field ***New Password***. Repeat entry in the field ***Retype to Confirm***. Click on **OK** to save the setting.

Note

Make a note of the new password. Otherwise you can no longer access the **W500** user interface. Should you ever forget the password, you can revalidate the preset password. Press the reset button on the back of **W500** for at least three seconds. Then all the previous configuration steps also have to be performed again.

On this page you can check the current status and the general settings for **W500**.

3.3.2 Configuration File

On this page you can back up the current settings to a file or restore on the basis of the file.

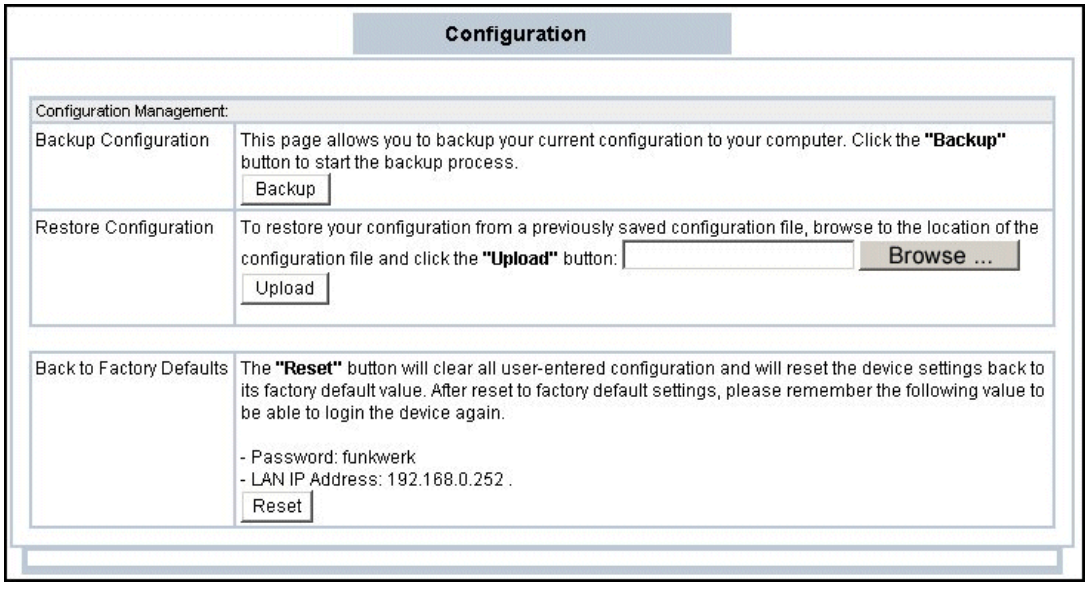

Configuration
Configuration Management:
Backup Configuration
This page allows you to backup your current configuration to your computer. Click the "Backup" button to start the backup process.
Backup
Restore Configuration
To restore your configuration from a previously saved configuration file, browse to the location of the configuration file and click the "Upload" button:
Browse ...
Upload
Back to Factory Defaults
The "Reset" button will clear all user-entered configuration and will reset the device settings back to its factory default value. After reset to factory default settings, please remember the following value to be able to login the device again.
- Password: funkwerk
- LAN IP Address: 192.168.0.252 .
Reset

Figure 3-12: Configuration

BACKUP CONFIGURATION: Backup the current configuration to the computer.

RESTORE CONFIGURATION: Restore the configuration from a previously saved configuration file.

BACK TO FACTORY DEFAULTS: The Reset button clears all user-entered configuration settings and resets the device back to its factory default settings.

- ***PASSWORD:*** *funkwerk*
- ***LAN IP ADDRESS:*** *192.168.0.252*

3.3.3 Upgrade Firmware

On this page you can upgrade the firmware via the Web.

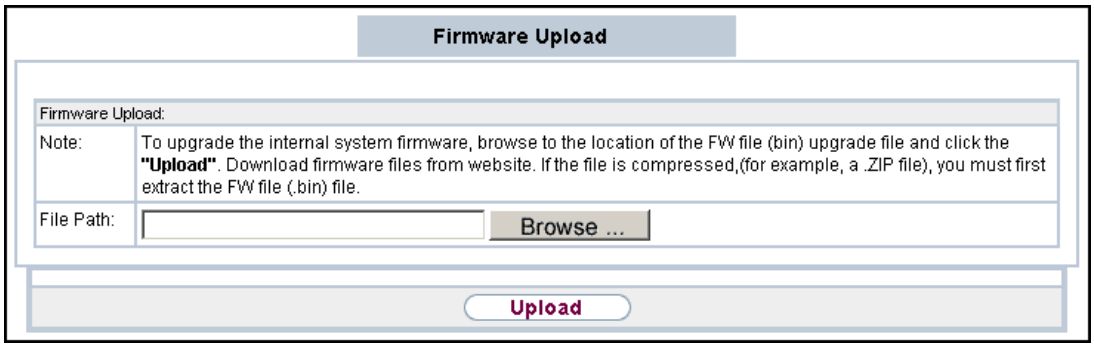

Firmware Upload
Firmware Upload:
Note:
To upgrade the internal system firmware, browse to the location of the FW file (bin) upgrade file and click the "Upload". Download firmware files from website. If the file is compressed,(for example, a .ZIP file), you must first extract the FW file (.bin) file.
File Path:
Browse ...
Upload

Figure 3-13: Firmware Import

With Firmware Import you can update the **W500** firmware to the latest version.

Please ensure that you have downloaded the latest and correct firmware from the product support website and have saved it to a local drive before you undertake the upgrade of the **W500** firmware.

To upgrade to the latest firmware, localize the file by clicking the button **Search** and then clicking **Upload** to start the upgrade process. Upgrading the firmware takes around seven minutes. If the firmware upgrade fails, repeat the steps described above.

Warning!

Never switch off the device during the upgrade. The result of interrupted upgrading operations could be that your gateway no longer boots.

3.4 Monitoring

3.4.1 Logs

You can view log entries and alarm messages on the screen. As soon as the log table is full, new log entries replace the oldest entries.

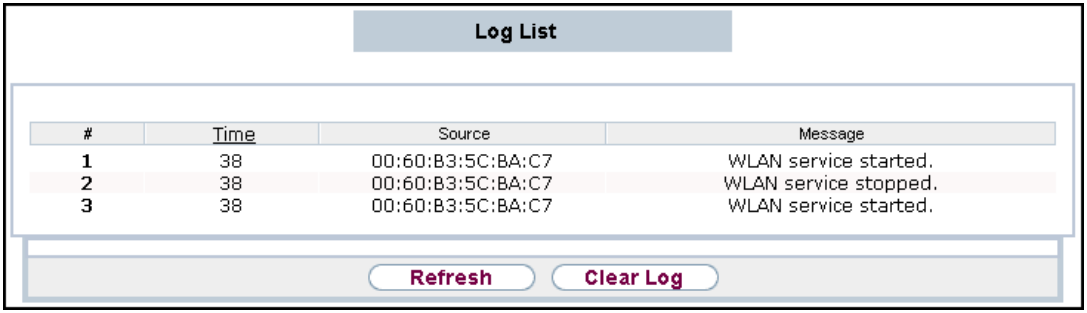


Figure 3-14: Log List

Click **Refresh** to update the log table.

Click **Clear Log** to delete all the entries.

3.4.2 Statistics

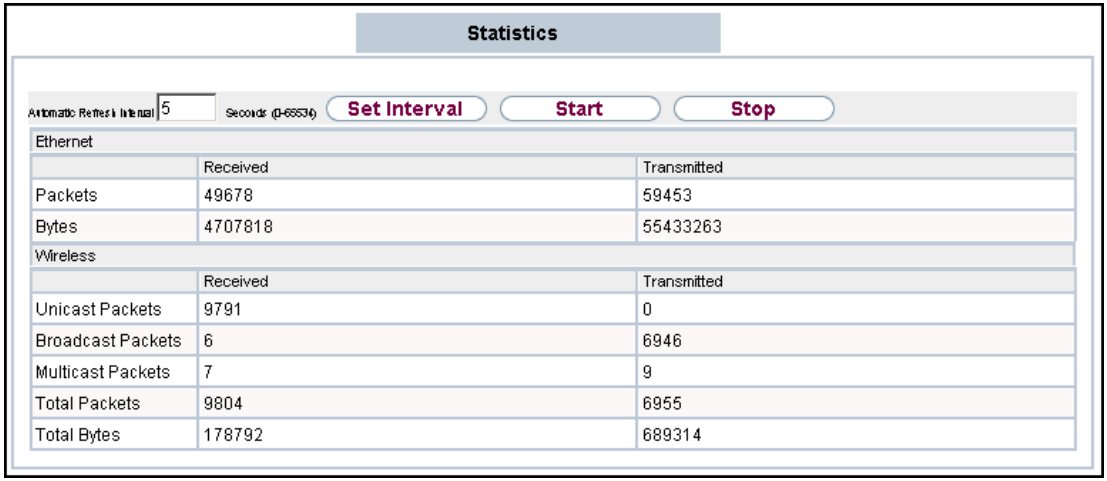


Figure 3-15: Statistics

The ***AUTOMATIC REFRESH INTERVAL*** specifies after how many seconds the display of statistical information is refreshed. **Set Interval** changes the number of seconds depending on the entry; **Stop** halts the refreshing process.

Under ***ETHERNET*** the number of packets or bytes sent or received via the RJ45 Ethernet interface is displayed.

Under ***WIRELESS*** the number of packets or bytes sent or received via the WLAN Radio interface is displayed as a total sum and also itemized in parts *Unicast* (one to one), *Broadcast* (one to all) and *Multicast* (one to several).

3.4.3 List of Associated Devices

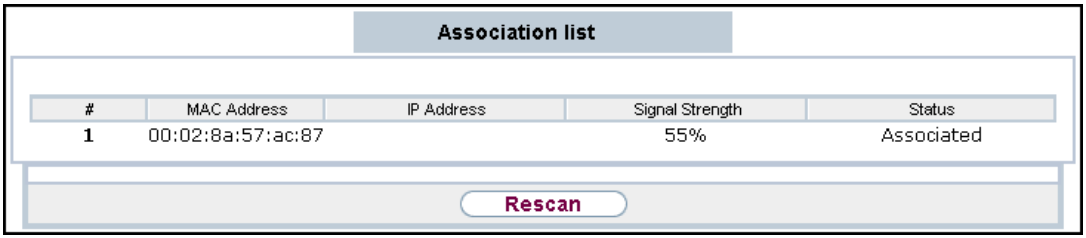


Figure 3-16: List of Associated Devices

The list of associated devices (***ASSOCIATION LIST***) shows those WLAN clients that are connected to the SSID of the AP.

The list displays the serial number (#), the MAC address of the WLA client (***MAC ADDRESS***), the IP address of the WLA client (***IP ADDRESS***), the signal strength of the wireless connection in percent (***SIGNAL STRENGTH***) and the ***STATUS*** of the WLAN client to the SSID of the AP (normally *Associated*).

4 Use of the Device in Various Network Scenarios

W500 can be used for different network scenarios, as described below.

4.1 Bridge Mode with WEP

In bridge mode, two W500s are linked together and this connection is used to couple two LANs. The two W500s in bridge mode do not offer an access point function, i.e. no clients can be connected with the W500s in bridge mode.

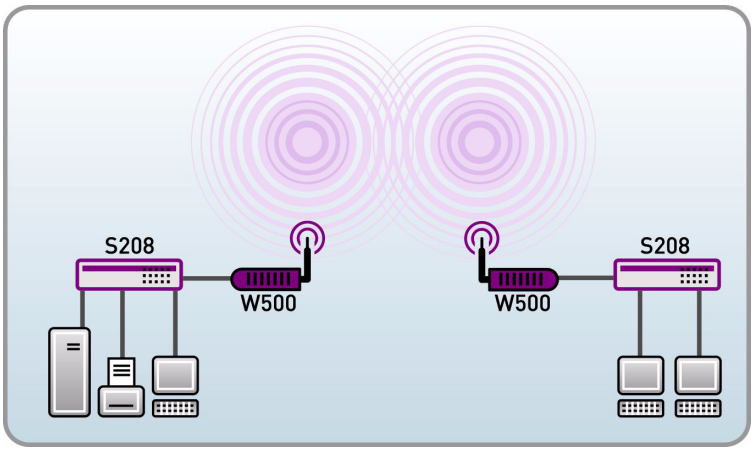


Figure 4-1: Bridge mode

4.1.1 Login

To establish the connection with the web browser, log in with user name and password (the standard IP address is *192.168.0.252*, the standard user name is *admin* and the standard password is *funkwerk*). The language can also be selected on the Login page (*English* or *German*).

Figure 4-2: Login

4.1.2 Navigation Menu

The initial setting is made in ***WIRELESS LAN - WIRELESS SETTINGS***. Figure 4-3 shows the navigation menu from the left section of the screen.

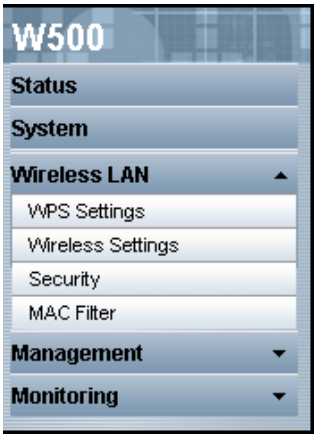


Figure 4-3: Navigation bar

4.1.3 Setting Operation Mode

Here (***WIRELESS LAN - WIRELESS SETTINGS***) **W500** is assigned the ***OPERATION MODE*** *Bridge*.

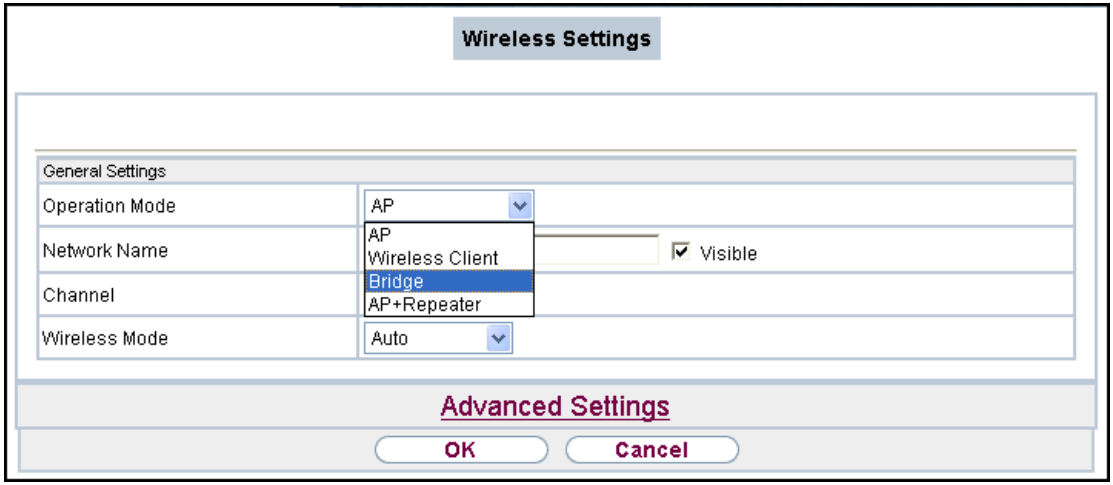


Figure 4-4: Setting Operation Mode

4.1.4 Advanced Settings / Setting MAC Address

After setting the ***CHANNEL*** and activating ***RADIO*** (***ADVANCED SETTINGS***) the MAC address of the second bridge, with which the connection is to be established, has to be specified. In turn, the bridge mode is also selected on the second **W500** and the MAC address of the first bridge is specified. Confirm with **OK**.

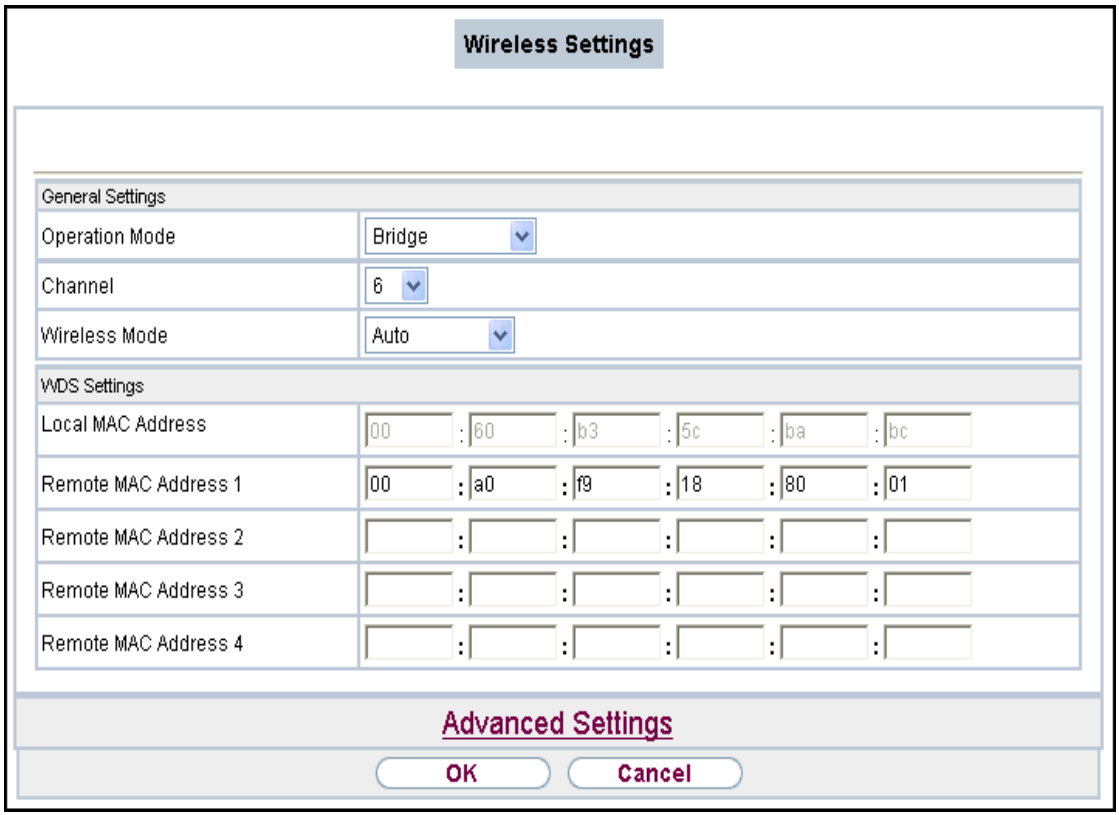


Figure 4-5: Entry of the MAC address

Setting the Security Mode.

Note

In bridge mode, only the security mode *WEP* is supported.

Configuration takes place in ***WIRELESS LAN - SECURITY***. In Figure 4-6 configuration with *WEP* is shown. After selecting the security mechanism, a freely select-

able WEP key (default key is ***WEP KEY 1***) must be configured. Follow the instructions on the screen. Confirm with **OK**.

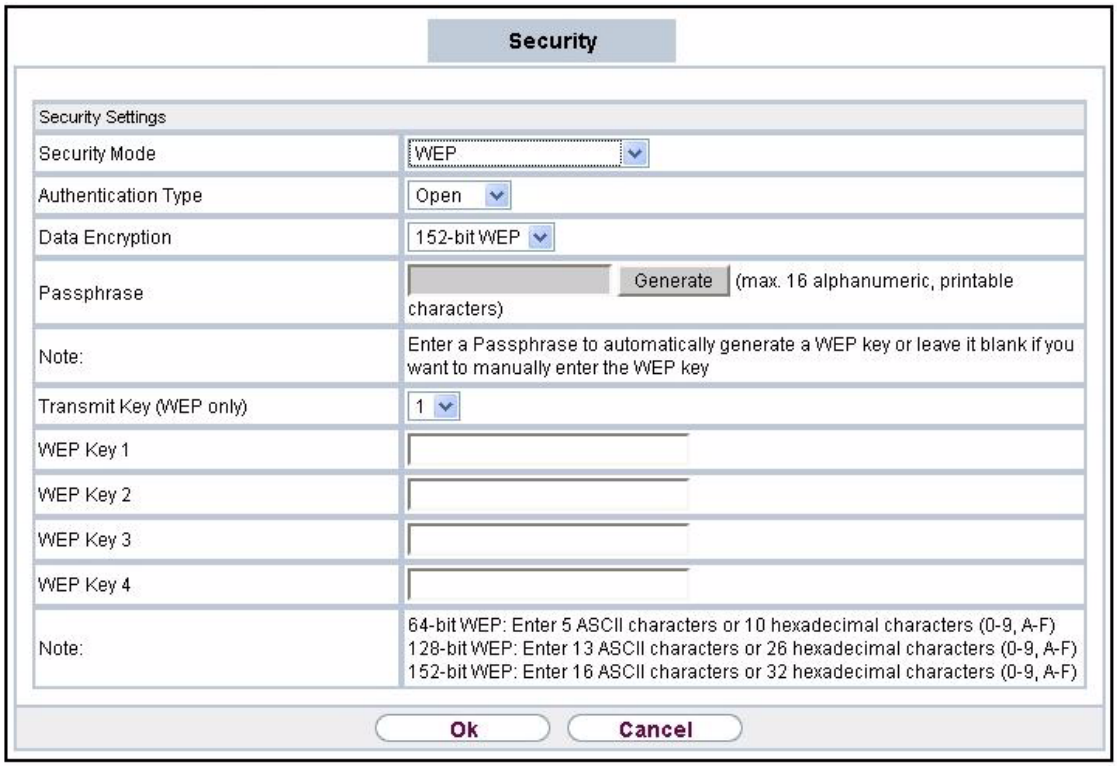

Security
Security Settings
Security Mode
WEP
Authentication Type
Open
Data Encryption
152-bit WEP
Passphrase
Generate
(max. 16 alphanumeric, printable characters)
Note:
Enter a Passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key
Transmit Key (WEP only)
1
WEP Key 1
WEP Key 2
WEP Key 3
WEP Key 4
Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)
152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters (0-9, A-F)
Ok
Cancel

Figure 4-6: Security Mode

4.1.5 Checking Status

On the Status page (menu item ***STATUS*** in the navigation bar) the operation mode entries and the WLAN status show that the configuration of the bridge and establishment of the connection to the second bridge was successful.

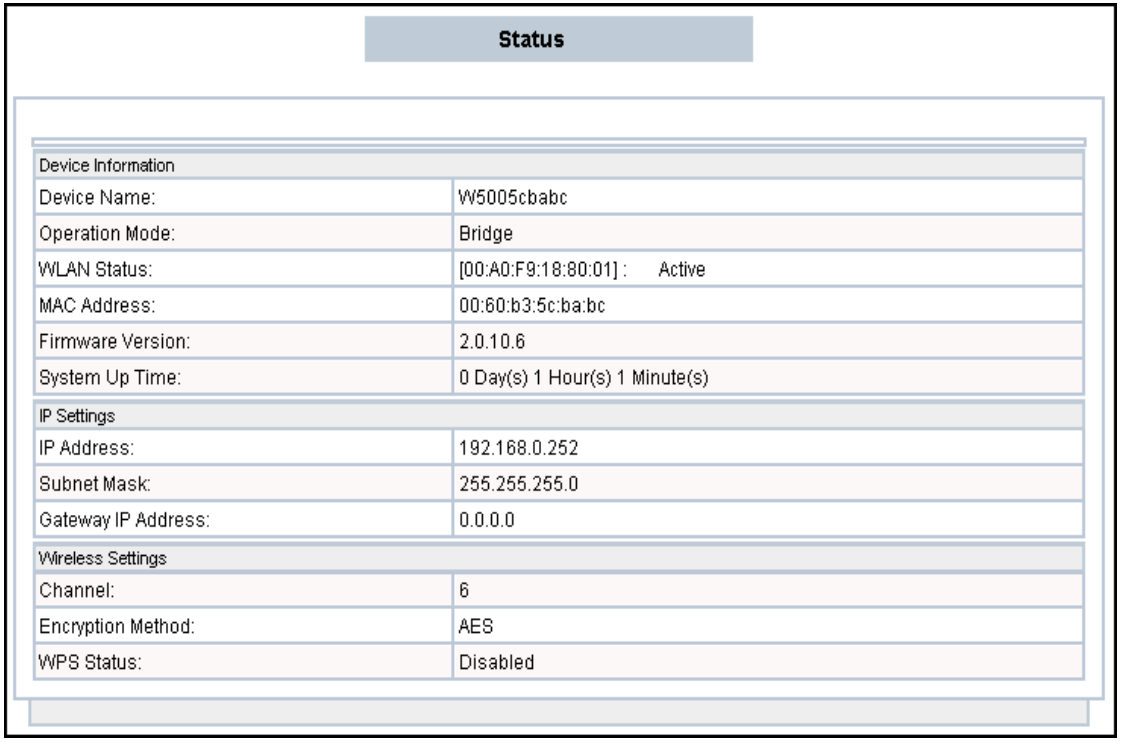


Figure 4-7: Status

4.2 Access Point Mode with WPA2-PSK and MAC Filter

In this mode clients are connected via WLAN to the access point. They can then communicate with other WLAN clients or clients in the wired LAN.

Note

Windows XP as a client operating system requires at least SP2 and update KB 893357 for WPA2.

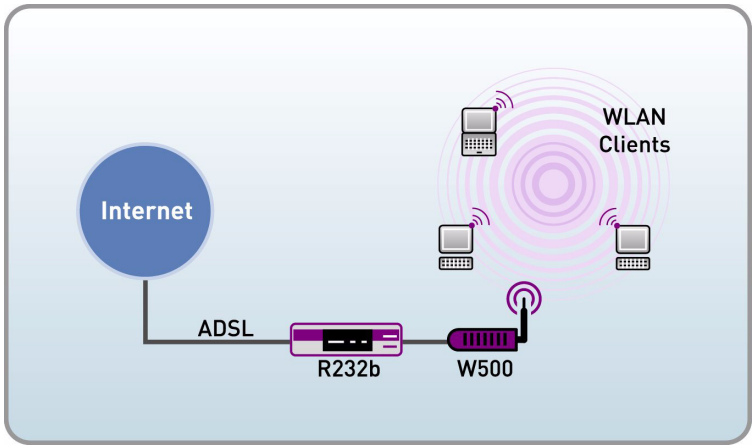


Figure 4-8: Access point mode

4.2.1 Login

For configuration, firstly the Web interface of the access point is called up with the aid of the browser and login is performed with user name and password. The standard IP address is *192.168.0.252*, the standard user name *admin* and the standard password *funkwerk*. The language can also be selected on the Login page (*English* or *German*).

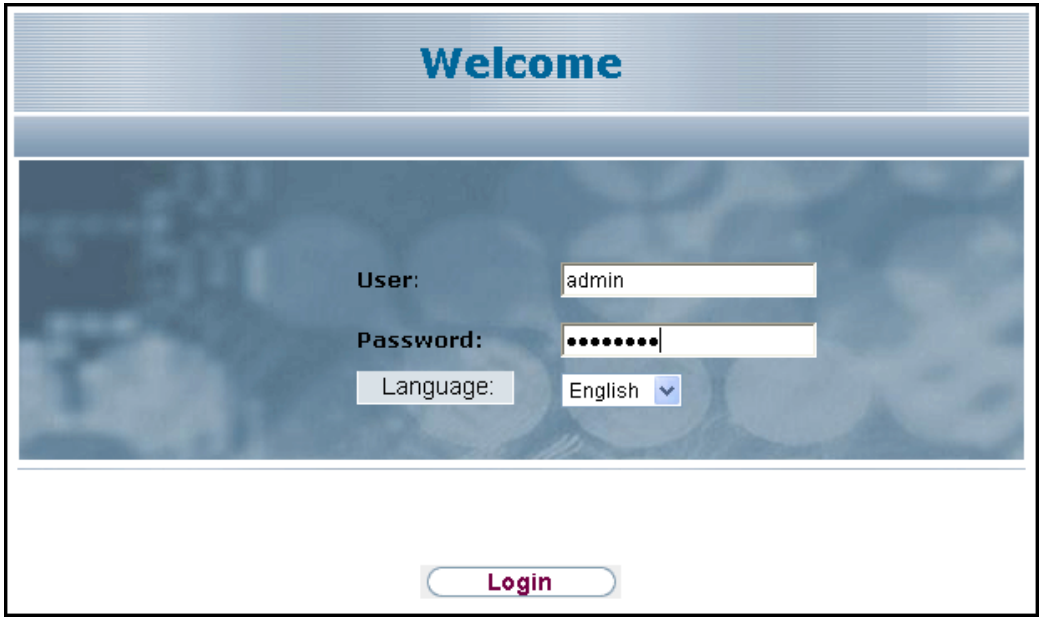


Figure 4-9: Login

4.2.2 Navigation Menu

In the menu on the left hand side in ***WIRELESS LAN*** the item ***WIRELESS SETTINGS*** is selected.

Figure 4-10: Navigation bar

4.2.3 Setting Operation Mode

The ***OPERATION MODE*** is selected as *AP*. The ***NETWORK NAME*** (SSID) must also be configured. This can be made visible or invisible. In Wireless Mode it can be determined whether *802.11b*, *802.11g* or both (*Auto*) are supported.

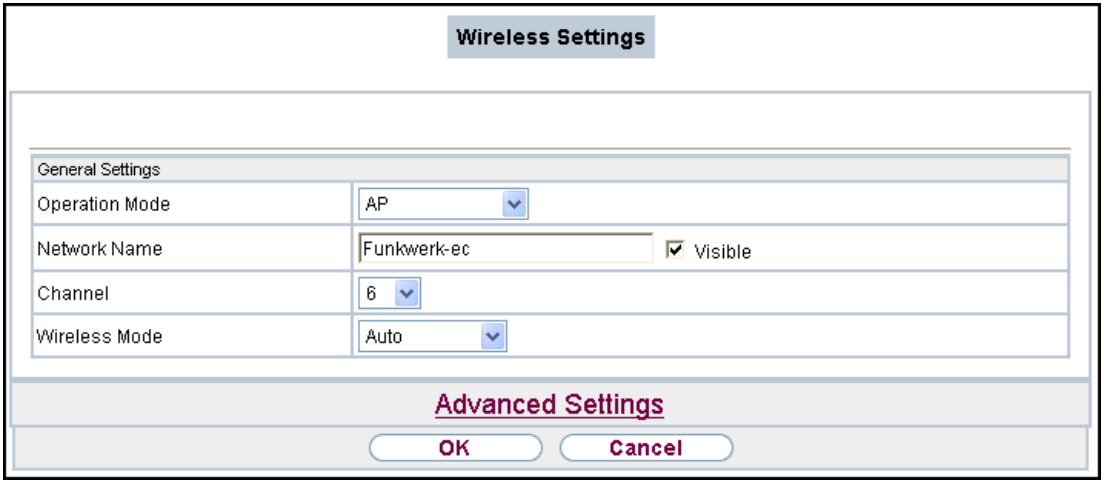


Figure 4-11: General settings

RADIO must be enabled in the ***ADVANCED SETTINGS***. On conclusion, confirm the entry with **OK**.

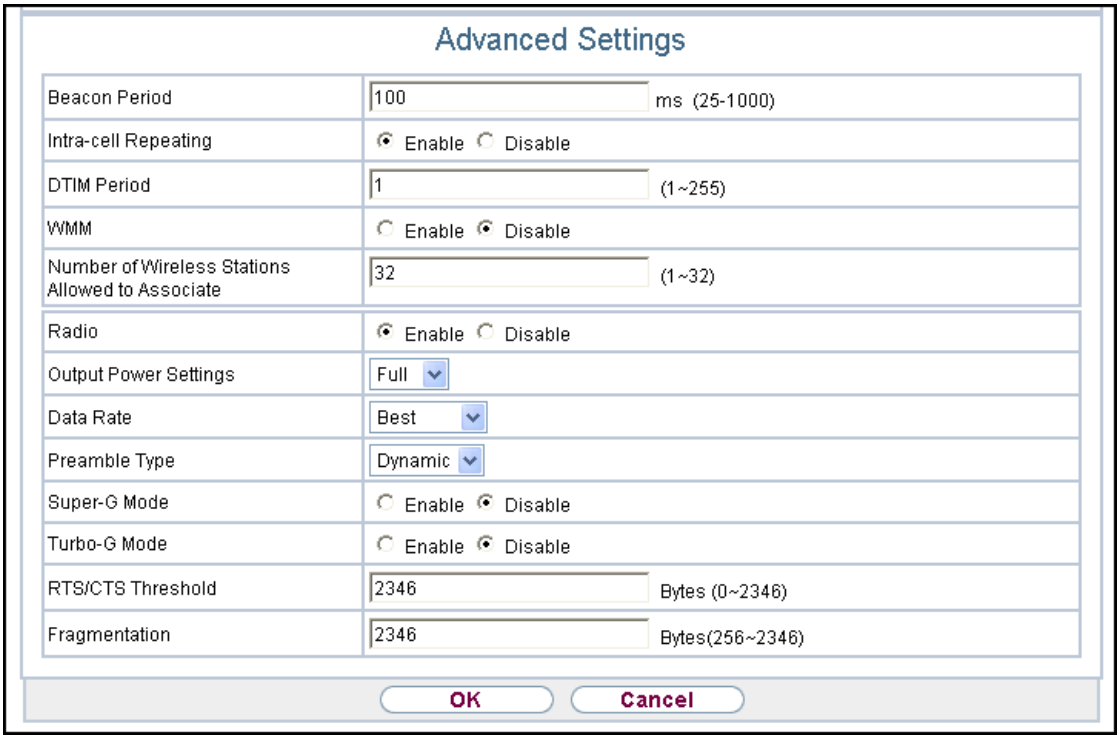


Figure 4-12: Enabling Radio

4.2.4 Setting the Security Mode

In order to achieve an encrypted WLAN connection to the clients, the encryption type must be selected in the Security menu item. In this example, the encryption method *WPA2-PSK* is selected.

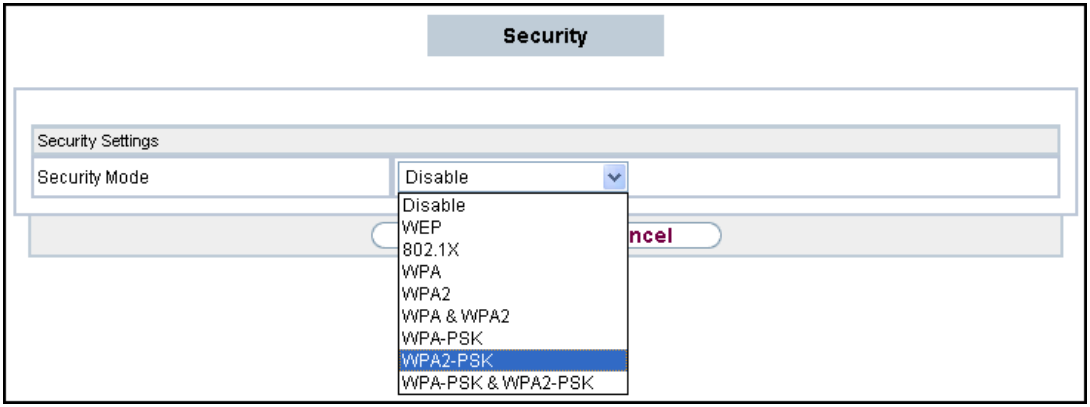


Figure 4-13: Security mode

Next of all, enter the freely selectable ***PRE-SHARED KEY***. The key must also be entered for the relevant clients. The maximum length of 63 ASCII characters should be fully exploited to make the key as secure as possible. On conclusion, confirm the entry with **OK**.

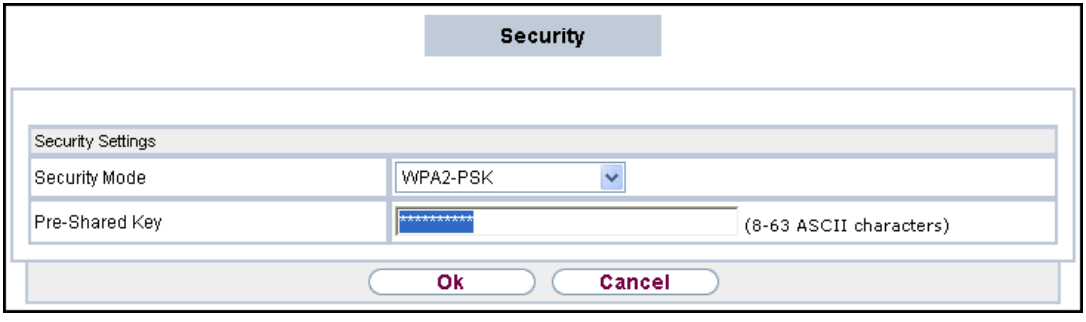


Figure 4-14: Pre-shared key

Configuration of a MAC address filter takes place in ***WIRELESS LAN - MAC FILTER***. Here the MAC address of a client that is allowed to use the access point is now entered. On conclusion, confirm the entry with **OK**.

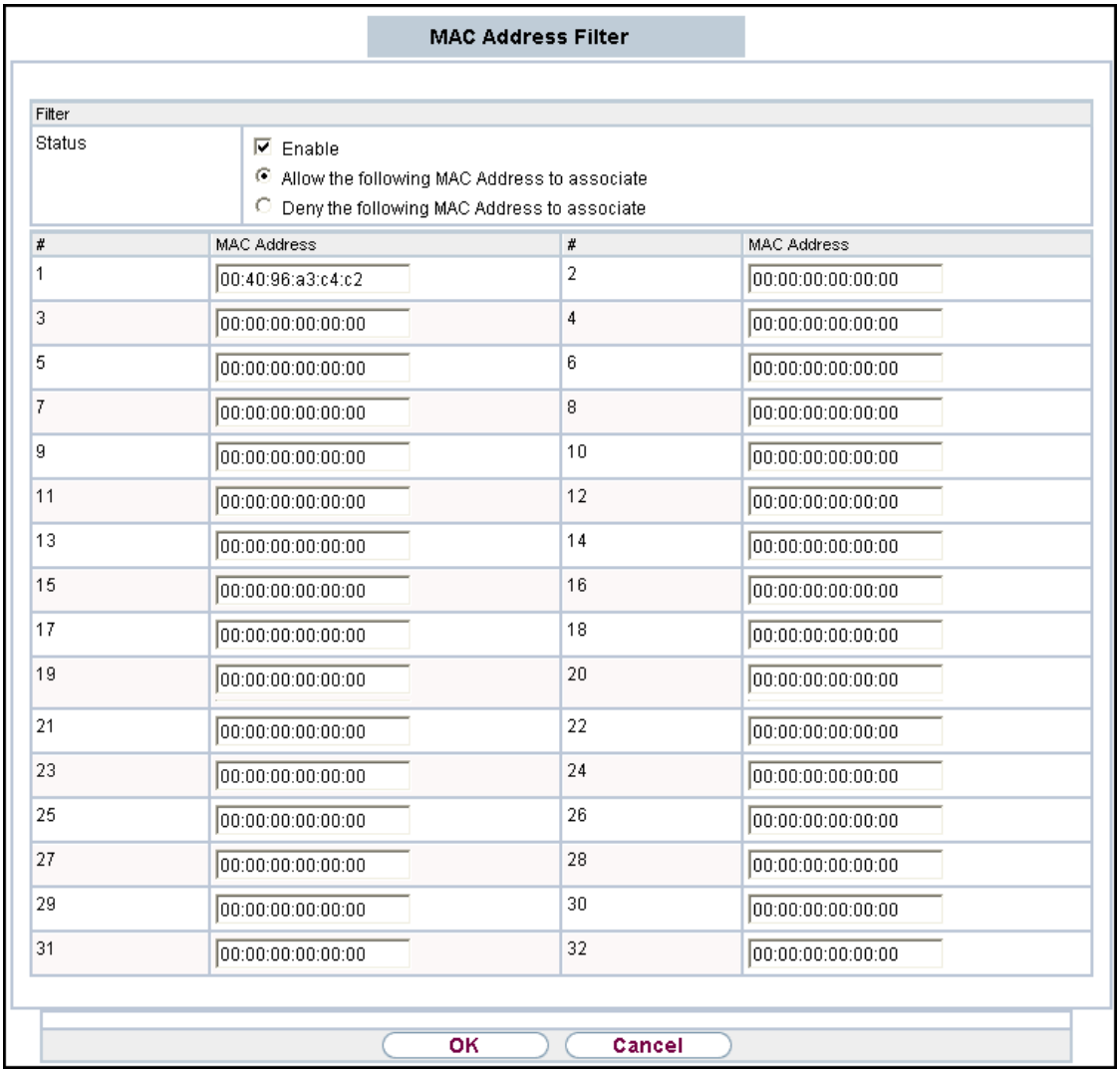


Figure 4-15: MAC Address Filter

4.2.5 Checking Status

In the menu item ***MONITORING – ASSOCIATION LIST*** an entry for this device can be seen if a client is logged in.

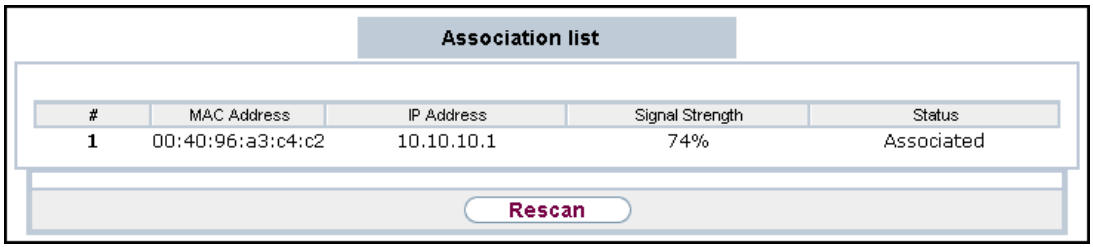


Figure 4-16: List of associated devices

The Status display offers the possibility of gaining an overview of the security configured.

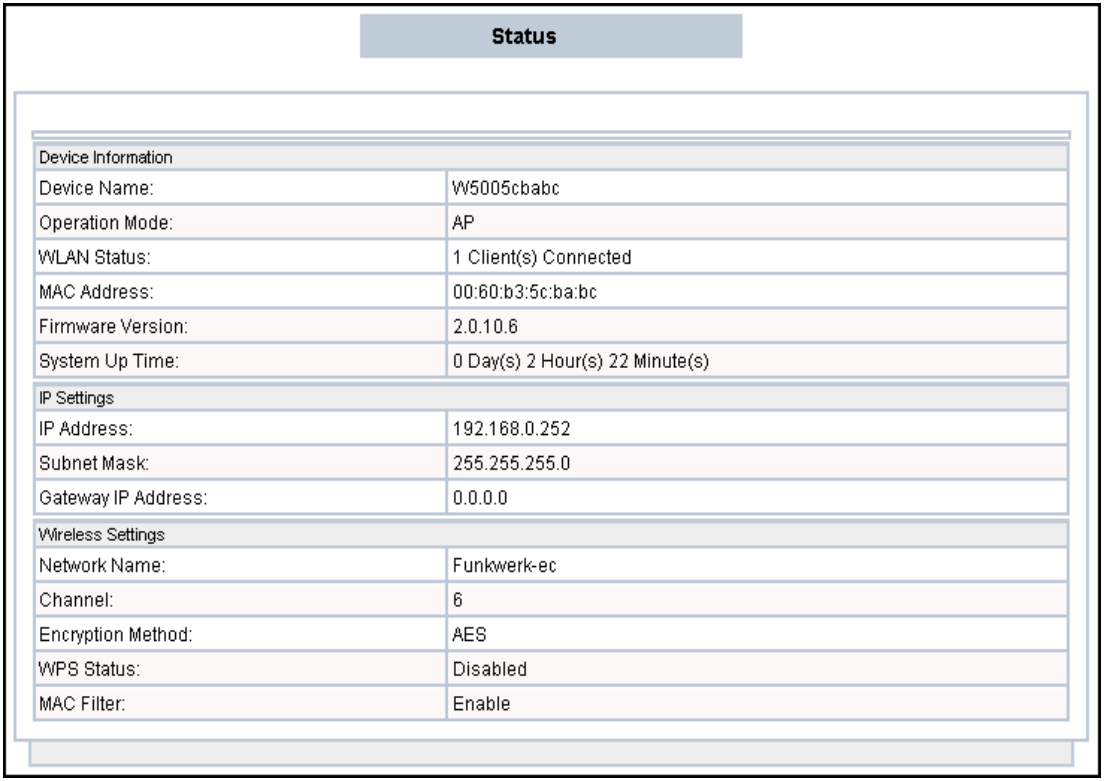


Figure 4-17: Status

4.3 AP + Repeater Mode with WPA2-PSK

This scenario offers the possibility of expanding a wireless cell with a second **W500**. Both access points are set to the "AP+Repeater" mode. The two devices are connected together via WLAN and at the same time provide their WLAN interface for connecting clients.

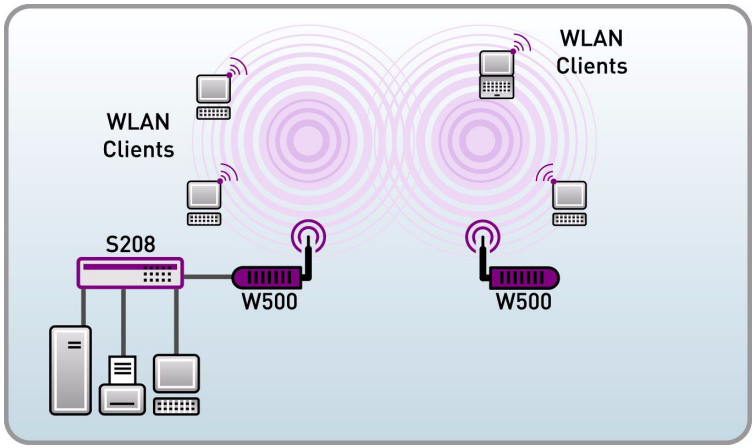


Figure 4-18: AP + Repeater mode

4.3.1 Login

The connection to **W500** is established with a browser. The standard IP address is *192.168.0.252*, the standard user name *admin* and the standard password *funkwerk*. The language can also be selected on the Login page (*English* or *German*).

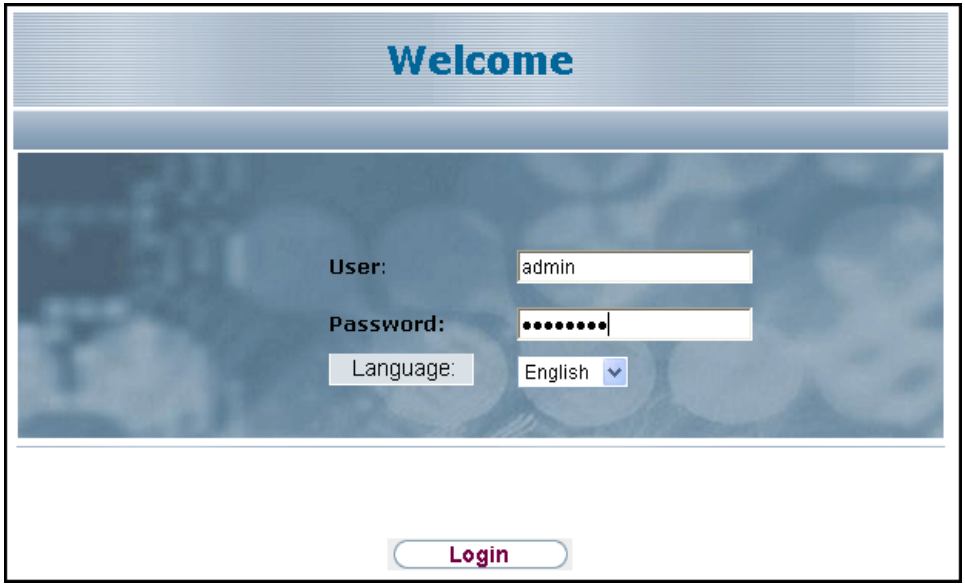


Figure 4-19: Login

4.3.2 Navigation Menu

Configuration starts in ***WIRELESS LAN - WIRELESS SETTINGS***.

Figure 4-20: Navigation bar

4.3.3 Setting Operation Mode

The ***OPERATION MODE*** is selected as *AP+Repeater*.

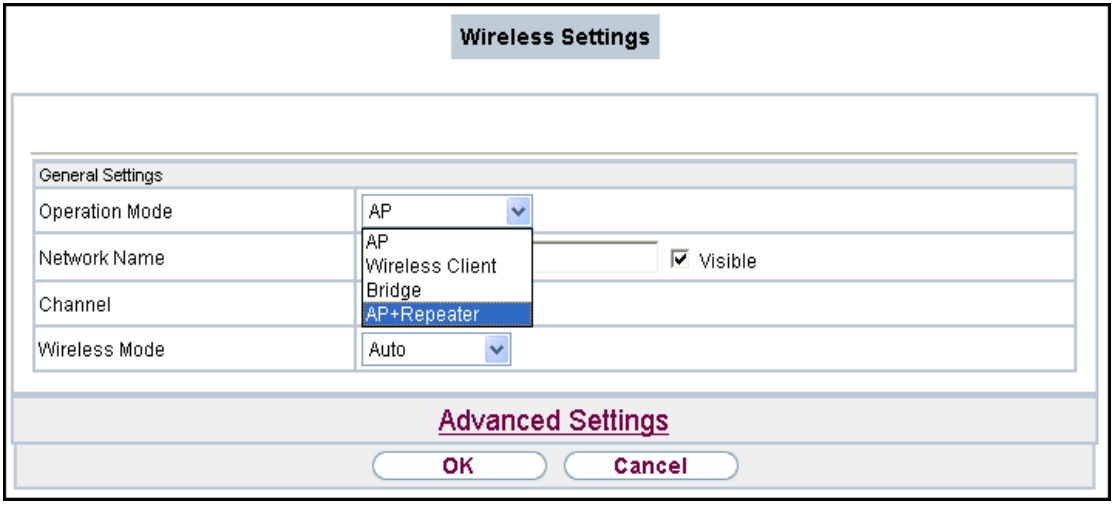


Figure 4-21: Setting Operation Mode

Besides configuring the ***CHANNEL*** and enabling ***RADIO***, the MAC address of an access point is also entered, which acts as a repeater and is logged on to this access point. In turn, the MAC address of this access point must be entered at the second access point. This entry is confirmed with **OK**.

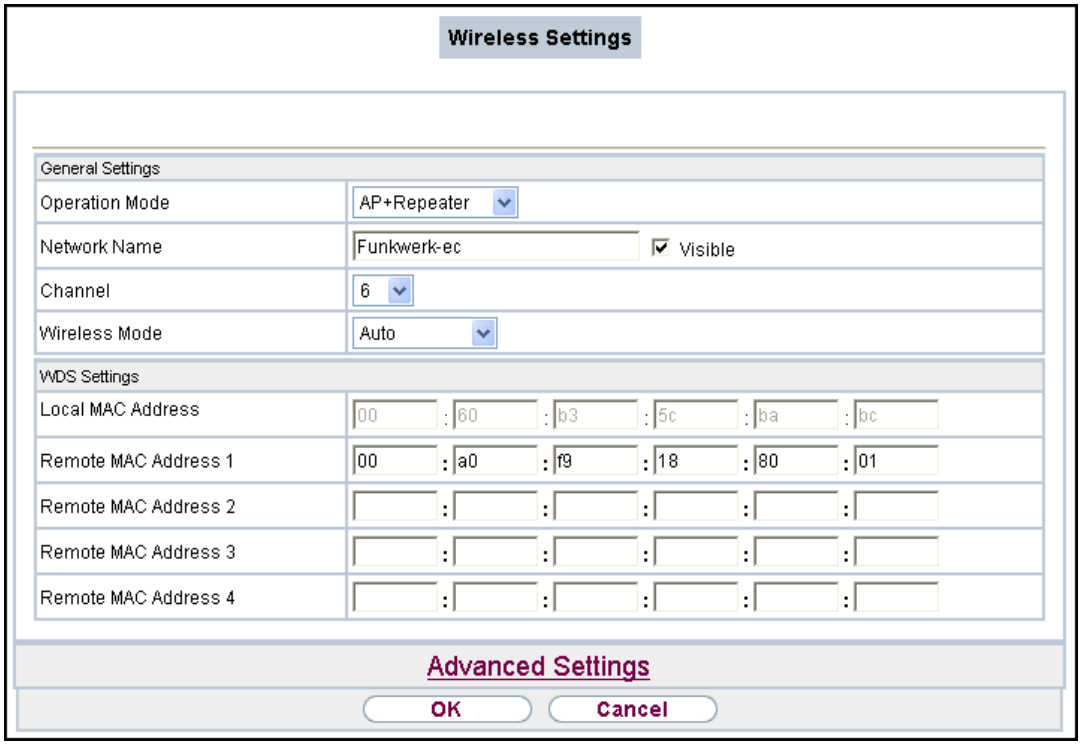


Figure 4-22: Further settings

4.3.4 Setting the Security Mode

For *AP+Repeater* mode, the security selection can be made in the ***WIRELESS LAN - SECURITY*** menu between *WEP* and *WPA2-PSK*. A freely selectable PSK must be specified for WPA2-PSK, which also has to be entered on the opposite side. Confirm entry with **OK**.

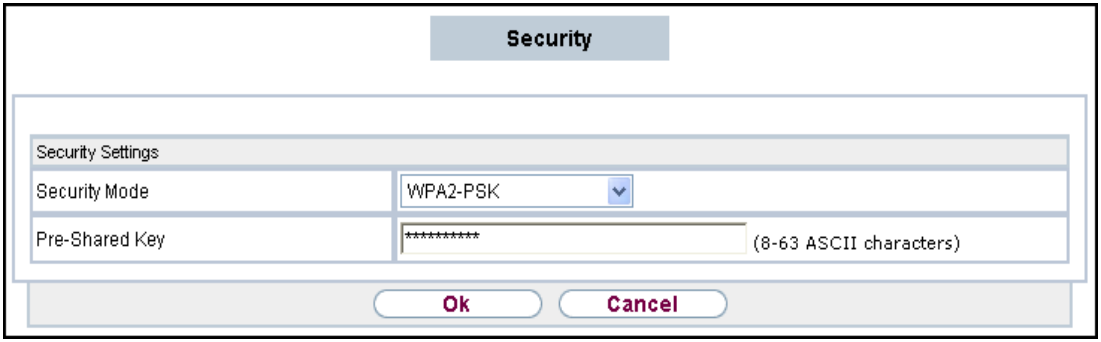


Figure 4-23: Security Mode

4.4 Wireless Client Mode with WPA2-PSK

In this scenario, a **W500** is configured as a client and can log on at a central AP as such. A PC can be connected to the wireless client, which can use the wireless client AP as a WLAN interface, as it were.

Firstly a **W500** or another access point must be configured as an AP with a corresponding network name (SSID), channel settings and security. This takes place as in the AP mode scenario.

4.4.1 Login

For configuration, firstly the Web interface of the access point is called up with the aid of the browser and login is performed with user name and password. The standard IP address is *192.168.0.252*, the standard user name is *admin* and the standard password is *funkwerk*. The language can also be selected on the Login page (*English* or *German*).

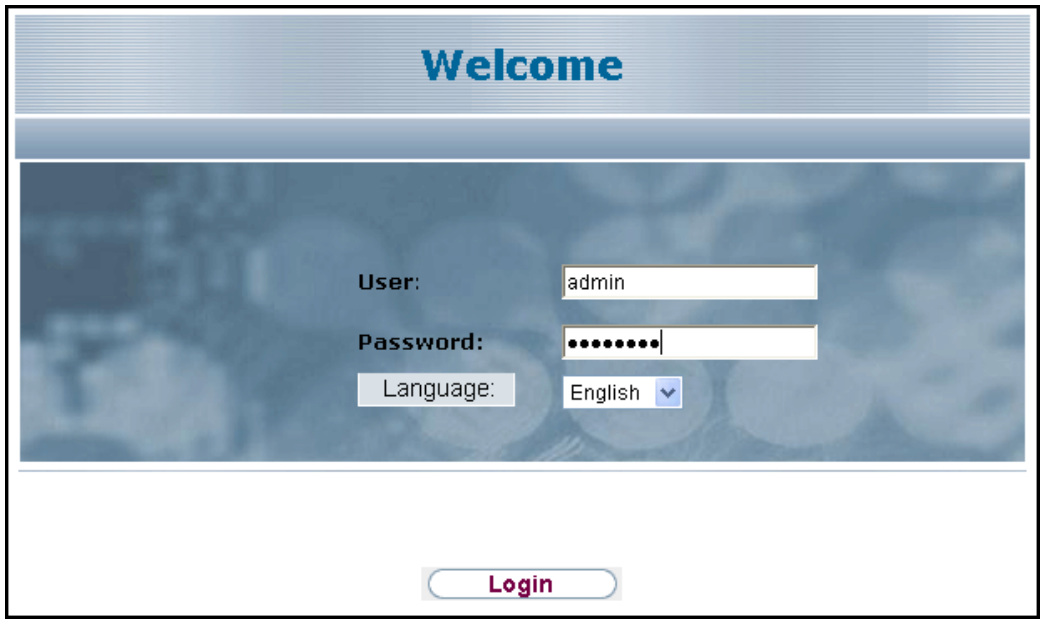


Figure 4-24: Login

4.4.2 Navigation Menu

In the menu on the left hand side in ***Wireless LAN*** the item ***Wireless Settings*** is selected.

Figure 4-25: Navigation bar

4.4.3 Setting Operation Mode

The ***OPERATION MODE*** is selected as *AP*. The ***NETWORK NAME*** (SSID) must also be configured. This can be made visible or invisible. In Wireless Mode it can be determined whether *802.11b*, *802.11g* or both (*Auto*) are supported.

.

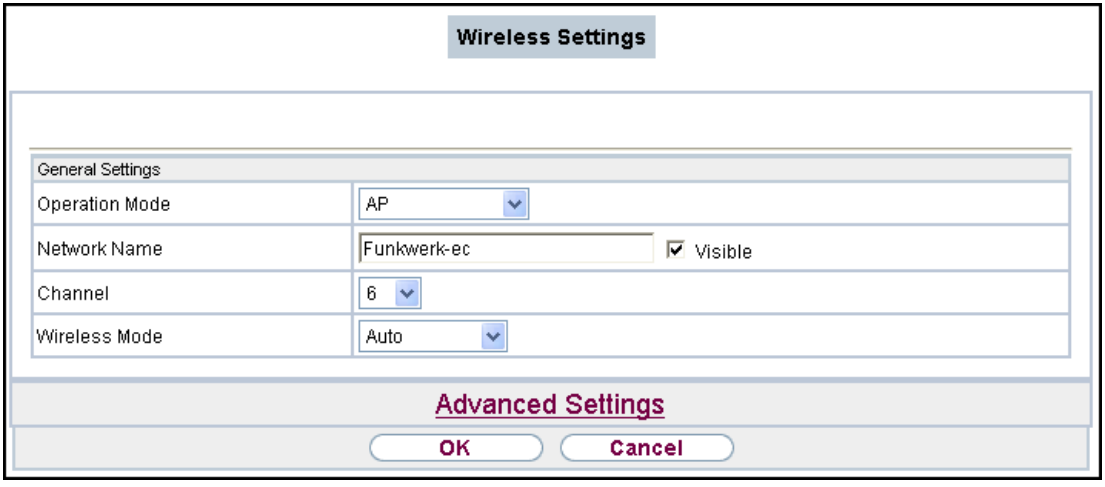


Figure 4-26: General settings

RADIO must be enabled in the ***ADVANCED SETTINGS***. On conclusion, confirm the entry with **OK**.

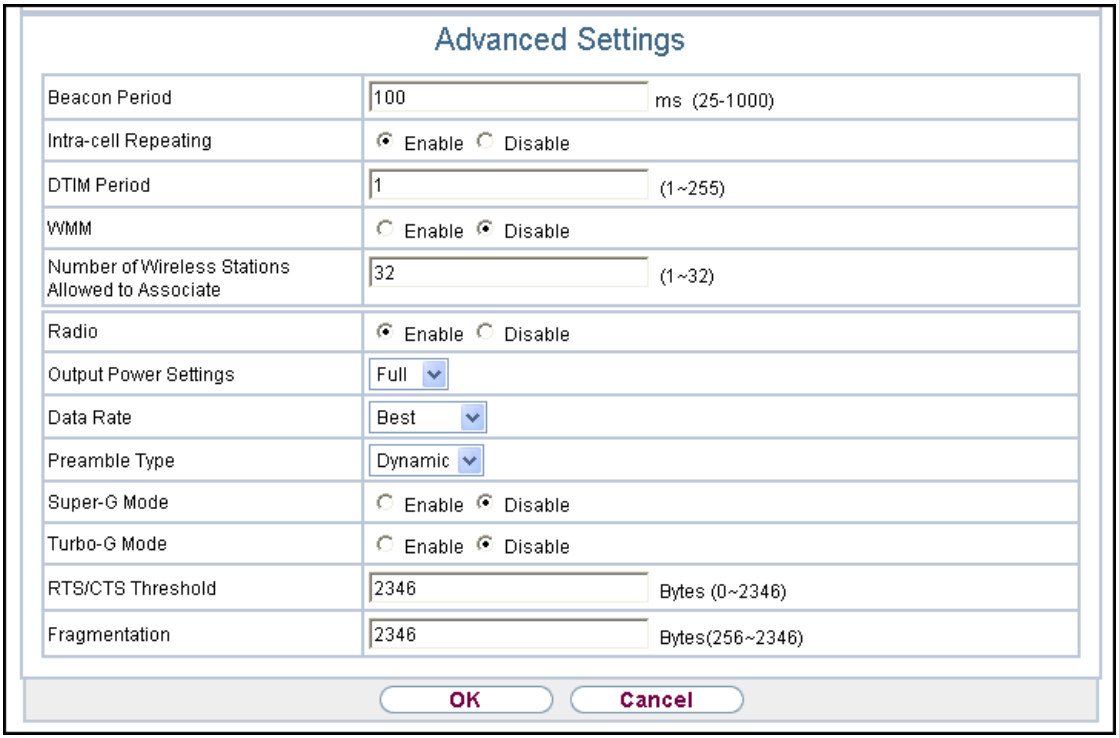


Figure 4-27: Enabling Radio

4.4.4 Wireless Client

Configuration of the wireless client begins with the menu item ***WIRELESS LAN - WIRELESS SETTINGS***. Here the mode *Wireless Client* must first be selected.

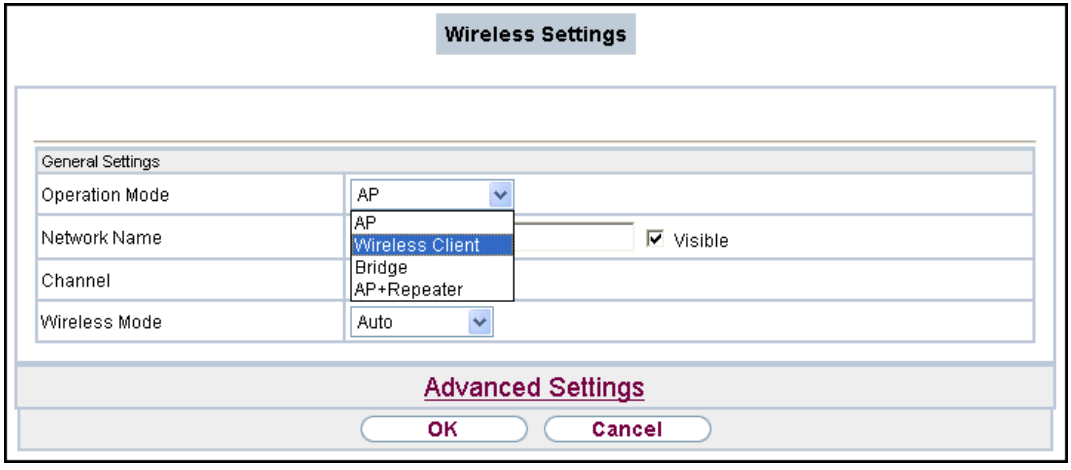


Figure 4-28: Operation Mode

Make sure that ***RADIO*** is enabled in the ***ADVANCED SETTINGS***.

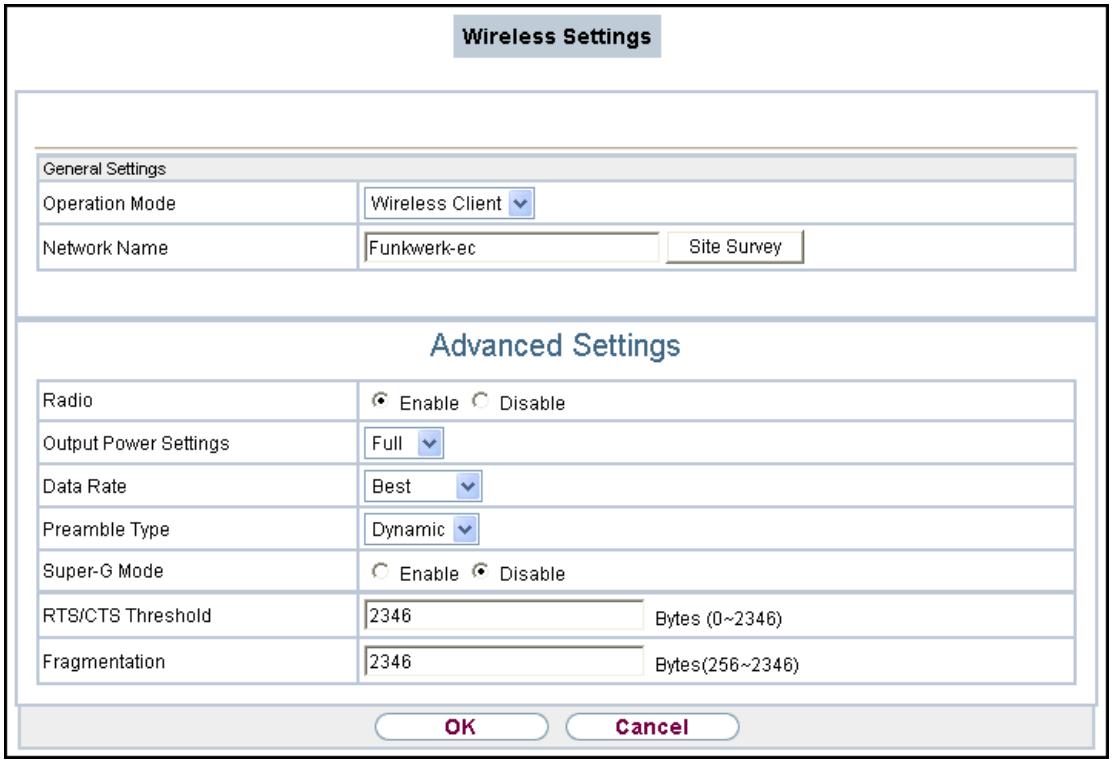


Figure 4-29: Activating the air interface

The ***NETWORK NAME*** (SSID) is then entered in the same window. The SSID of the client must correspond with the SSID of the access point to which the wireless client is to be connected. The entry must be confirmed with **OK**.

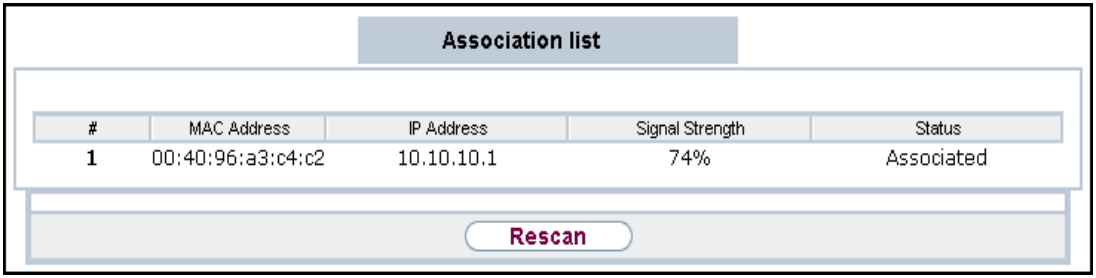


Figure 4-30: List of associated devices

4.4.5 Security Mode for the Wireless Client

The ***SECURITY MODE*** is entered in the next step. In our example, *WPA2-PSK* is used for security. In ***WIRELESS LAN - SECURITY*** the encryption type is selected and the ***PRE-SHARED KEY*** entered. At the end the entry is confirmed with **OK**.

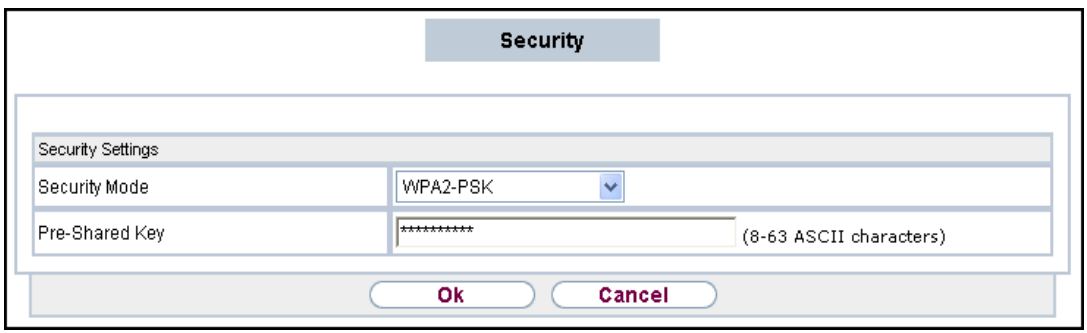


Figure 4-31: Security Mode

4.4.6 Checking the Client's Status

On the ***STATUS*** page it can be identified whether the wireless client is associated.

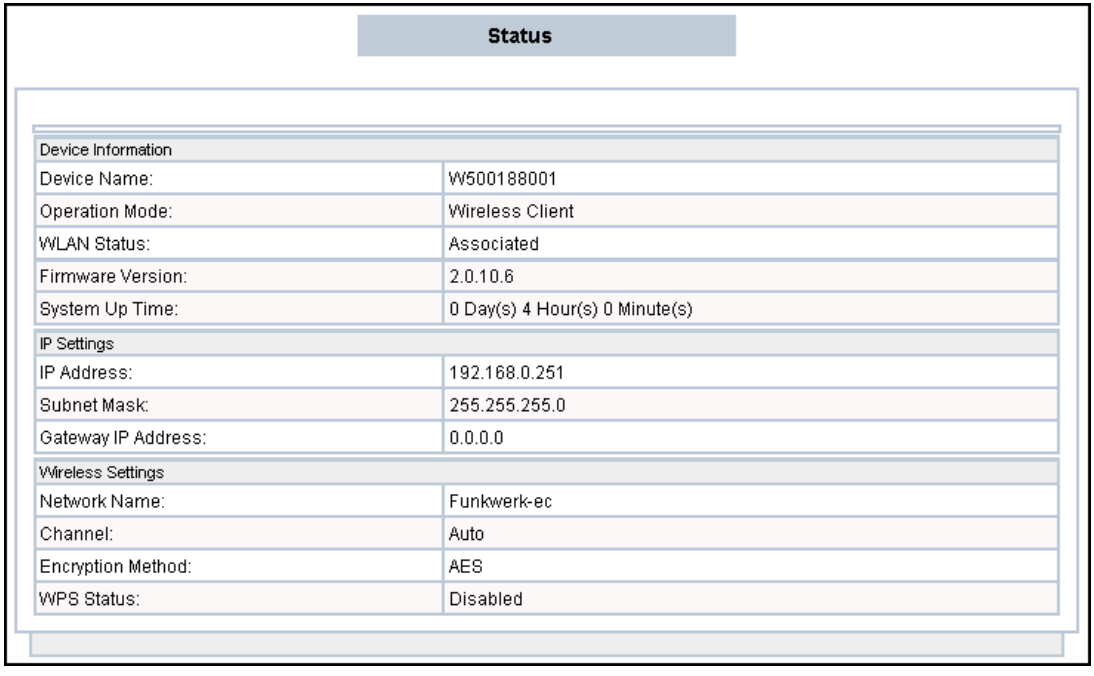


Figure 4-32: Checking Status

5 Warranty

The development and production process is subject to comprehensive quality management. This way we can offer our customers top quality products. We guarantee the quality of our products in accordance with the statutory warranty regulations. Warranty cases are handled by your contractual partner, i.e. your dealer or distributor.

The period of warranty coverage for **W500** is 24 months.

5.1 Replacement, Repair and Refund for Hardware

Should a power outage occur during a firmware upgrade or thereafter and functional faults result, please contact your supplier.

If the device has to be repaired or replaced, send it back to your suppler in the original packaging. You have to enclose the following documents with a defective device, which you send in during the warranty period.

- Warranty repair card
- Copy of the invoice or evidence of purchase and
- RMA report form. Request an RMA form (Return Materials Authorization) from your supplier.

After checking the purchasing slip, we will make our decision on repairing or replacing the defective part for the purchaser free of charge.

This warranty shall be granted under the condition that the product is used for the intended purpose and in an appropriate way. Products expressly excluded from the warranty are those modified without the consent of the manufacturer, subjected to extraordinary mechanical or electrical stresses or have been damaged in other ways.

Please fill out the following table and keep this information together with the product.

Name:	
Title:	
Company:	
Phone:	
Fax:	
e-mail:	
ZIP-Code/City:	
Country:	
Product name:	
Serial number:	
MAC address:	
Invoice date:	
Product description:	

Contact your authorized vendor in case of further questions.

5.2 Technical Data

PRODUCT DESCRIPTION:	IEEE 802.11g WLAN access point
ANTENNA:	Detachable 5dBi RSMA antenna
OUTPUT POWER:	14 dBm + 5 dBm antenna gain
SENSITIVITY:	11g @ PER 10% 54 Mbps <= -65 dBm; 11b @ PER 8% 11 Mbps <= -80 dBm
MODULATION:	11g (OFDM) 64QAM, 16QAM, QPSK, BPSK; 11b (DSSS) CCK, DQPSK, DBPSK
RANGE:	11g: 54 Mbps up to 60 meters, 11 Mbps up to 120 meters; 11b: 11 Mbps up to 80 meters, 1 Mbps up to 200 meters
FREQUENCY BAND:	Europe (ETSI) 13 channels: 2.412 GHz – 2.472 GHz
INTERFACE	A 10/100 Base-T Ethernet interface with Auto MDI(X) support
OPERATION MODES:	access point, repeater, bridge and wireless client
SECURITY:	WPA/WPA2, 802.1x, WEP 64/128/154-bit
DIMENSIONS:	110mm x 125mm x 30mm (LxWxH)
WEIGHT:	approx. 200g
TEMPERATURE RANGE:	Operation 0 to 50°C, storage -10 to 65°C
AIR HUMIDITY:	90% (not condensing)
WARRANTY:	24 months

Safety Precautions

Copyright © February 3, 2010 Funkwerk Enterprise Communications GmbH
Version 2.2

6.1 General Safety Precautions in English

The following sections contain safety precautions you are strongly advised to heed when handling your device.

Transport and storage

- Transport and store your gateway in its original packaging only or use another suitable packaging to protect the unit against impact and shock.
- Please observe the transport and storage instructions attached to the packaging.

Installation and initial operation

- Observe the information on the ambient conditions (cf. **Technical Data** and **Quick Install Guide**) before installing and operating your gateway.
- Please observe the respectively applicable framework conditions in your country for the installation of external ISDN basic accesses. If and when required, consult a technician who has the corresponding licence. Obtain information about the special requirements of national regulations, and observe these legal requirements for the installation.
- When the unit is moved from a colder environment into the workroom, condensation may occurr on the inside and outside of the unit. Allow the unit to adapt to the temperature and to dry out completely before starting up operation. Observe the environmental conditions rendered in the manual chapter titled **Technical Data**.
- Make sure that shockproof (Home Office) socket used for the installation is freely accessible. The mains plug has to be unplugged to disconnect the unit from the mains completely.
- Make sure that the value of the upstream fuses of the mains connection do not exceed 16 amps.
- Please check whether the rated voltage rendered on the typeplate of the power supply unit corresponds to the local power supply.
- In case of wall installation, please ensure that the screws are safely screwed into the wall and can carry the weight of the unit and the cables.
- Make sure that the antennas of local-area wireless network units are screwed down tightly.

- Please make sure you follow the correct cabling sequence as described in the **Quick Install Guide**.
- Please check whether the cable connections are correct - in particular the ISDN and LAN cables - before you start operating your gateway. The ISDN connection of your gateway must not be connected to the Ethernet connection of your PC or hub, and the LAN connection of your gateway must not be attached to your ISDN connection.
- Only use the cables enclosed or specified for cabling - as described in the manual. If you use other cables, Funkwerk Enterprise Communications GmbH shall not accept any liability for any damage occurring or for any adverse effects on the functions.
- Please arrange the cables in such a way that they are no hazard (danger of stumbling) and cannot be damaged.
- Do not connect, disconnect or touch the data transmission lines during thunderstorms.

Intended use and operation

- Your gateway is intended for use in an office environment. As a multi-protocol gateway, your gateway establishes WAN connections in keeping with the system configuration. In order to avoid extra charges, it is imperative to carefully monitor the unit.
- Your gateway meets the relevant safety regulations for IT equipment when used in an office environment. If you have any questions as to whether the gateway can be set up in the intended environment, please get in touch with your funkwerk dealer or with the funkwerk Customer Support Department.
- The intended operation of the unit in keeping with European standard EN 60950 shall be ensured only when the unit cover has been fitted (cooling, fire protection, radio interference suppression).
- The ambient temperature should not exceed +50 deg. Celsius. Avoid exposure to direct sunlight. Ensure sufficient cooling.
- Make sure no foreign objects (such as paper clips) or liquids get into the inside of the unit (electric shock, short-circuit).
- Make sure that ventilation slits and orifices of the unit are not blocked.

- In cases of an emergency (such as damaged housing or operating element, penetration of liquid or foreign objects), immediately interrupt the power supply at the socket and notify the Service Department.

Local-area wireless network

- When the radio components are switched on, do not move the gateway into the vicinity of inflammable gases or into a potentially explosive environment (such as paint shop) as the radio waves emitted may cause an explosion or fire.
- The reach of the radio link depends on environmental and ambient conditions.
- Data traffic by a wireless connection may permit unauthorised third parties to receive data. Depending on how critical the safety of the data transmitted by WLAN are, carry out the necessary steps to secure your radio network.

Cleaning and repair

- The unit may be opened by trained specialist staff only. For this reason, repairs of the unit should be carried out only by a service centre authorised by funkwerk. Your dealer will tell you where the service centre is located. Unauthorised opening and improper repairs may result in considerable hazards for the user (such as electric shock). Unauthorised opening of the unit shall void guarantee and liability of Funkwerk Enterprise Communications GmbH.
- Never use any water or liquid to clean the unit. Penetrating water may cause considerable hazards for the user (such as electric shock) and considerable damage to the unit.
- Never use scouring agents, alkaline detergents, acidic or abrasive agents.

6.2 Allgemeine Sicherheitshinweise in Deutsch

In den nachfolgenden Abschnitten finden Sie Sicherheitshinweise, die Sie beim Umgang mit Ihrem Gerät unbedingt beachten müssen.

Transport und Lagerung

- Transportieren und lagern Sie Ihr Gateway nur in der Originalverpackung oder in einer anderen geeigneten Verpackung, die Schutz gegen Stoß und Schlag gewährt.
- Beachten Sie die an der Verpackung angebrachten Transport- und Lagerhinweise.

Aufstellen und in Betrieb nehmen

- Beachten Sie vor dem Aufstellen und Betrieb Ihres Gateways die Hinweise für die Umgebungsbedingungen (vgl. **Technische Daten** und **Kurzanleitung**).
- Beachten Sie bei der Installation externer ISDN-Basisanschlüsse die jeweils gültigen Rahmenbedingungen Ihres Landes. Gegebenenfalls ist ein Techniker erforderlich, der über die entsprechende Zulassung verfügt. Informieren Sie sich über die Besonderheiten nationaler Verordnungen und beachten Sie deren rechtliche Grundlagen bei der Installation.
- Wenn das Gerät aus kalter Umgebung in den Betriebsraum gebracht wird, kann Betauung sowohl am Geräteäußeren als auch im Geräteinneren auftreten. Warten Sie, bis Ihr Gerät temperaturangeglichen und absolut trocken ist, bevor Sie es in Betrieb nehmen. Beachten Sie die Umweltbedingungen im Handbuchkapitel **Technische Daten**.
- Stellen Sie sicher, dass die Schutzkontakt-Steckdose der Installation frei zugänglich ist. Zur vollständigen Netztrennung muß der Netzstecker gezogen werden.
- Stellen Sie sicher, dass der Wert der vorgelagerten Sicherungen des Netzanschlusses 16 A nicht überschreiten.
- Überprüfen Sie, ob die auf dem Typenschild des Netzteils angegebene Nennspannung mit der örtlichen Netzspannung übereinstimmt.

- Bei Wandmontage stellen Sie sicher, dass die Schrauben sicher in der Wand verschraubt sind und das Gewicht des Gerätes und der Verkabelung tragen können.
- Achten Sie darauf, dass bei Funk-LAN-Geräten die Antennen fest verschraubt sind.
- Beachten Sie beim Verkabeln die Reihenfolge, wie in der **Kurzanleitung** beschrieben.
- Überprüfen Sie, ob Sie die Verkabelung – insbesondere die ISDN- und LAN-Verkabelung – richtig durchgeführt haben, bevor Sie Ihr Gateway in Betrieb nehmen. Der ISDN-Anschluß Ihres Gateways darf nicht mit dem Ethernet-Anschluß Ihres Rechners oder Hubs verbunden werden, der LAN-Anschluß Ihres Gateways nicht mit Ihrem ISDN-Anschluß.
- Verwenden Sie für die Verkabelung – wie im Handbuch beschrieben – nur die beigelegten bzw. spezifizierten Kabel. Falls Sie andere Kabel verwenden, übernimmt Funkwerk Enterprise Communications GmbH für auftretende Schäden oder Beeinträchtigung der Funktionalität keine Haftung.
- Verlegen Sie Leitungen so, dass sie keine Gefahrenquelle (Stolpergefahr) bilden und nicht beschädigt werden.
- Schließen Sie Datenübertragungsleitungen während eines Gewitters weder an noch ziehen Sie sie ab oder berühren Sie diese.

Bestimmungsgemäße Verwendung, Betrieb

- Ihr Gateway ist für den Einsatz in einer Büroumgebung bestimmt. Als Multiprotokoll-Gateway baut Ihr Gateway in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen.
- Ihr Gateway entspricht den einschlägigen Sicherheitsbestimmungen für Einrichtungen der Informationstechnik für den Einsatz in einer Büroumgebung. Falls Sie Fragen haben, ob Sie das Gateway in der vorgesehenen Umgebung aufstellen können, wenden Sie sich bitte an Ihren funkwerk Händler oder an den funkwerk Customer Support.

- Der bestimmungsgemäße Betrieb des Systems gemäß EN 60950 ist nur bei montiertem Gehäusedeckel gewährleistet (Kühlung, Brandschutz, Funkentstörung).
- Die Umgebungstemperatur sollte 50 °C nicht übersteigen. Vermeiden Sie direkte Sonneneinstrahlung. Achten Sie auf ausreichende Kühlung.
- Achten Sie darauf, dass keine Gegenstände (z. B. Büroklammern) oder Flüssigkeiten ins Innere des Geräts gelangen (elektrischer Schlag, Kurzschluß).
- Stellen Sie sicher, dass die Lüftungsschlitze und -öffnungen des Gerätes nicht blockiert sind.
- Unterbrechen Sie in Notfällen (z. B. beschädigtes Gehäuse oder Bedienelement, Eindringen von Flüssigkeit oder Fremdkörpern) sofort die Stromversorgung an der Steckdose und verständigen Sie den Service.

Funk-LAN

- Bringen Sie das Gateway nicht mit eingeschalteter Funkkomponente in die Nähe entflammbarer Gase oder in eine explosionsgefährdete Umgebung (z. B. Lackiererei), da die übertragenen Funkwellen eine Explosion oder ein Feuer auslösen können.
- Die Reichweite der Funkverbindung ist abhängig von Umwelt- und Umgebungsbedingungen.
- Bei Datenverkehr über eine drahtlose Verbindung ist es auch unberechtigten Dritten möglich, Daten zu empfangen. Ergreifen Sie daher je nachdem, wie kritisch die Sicherheit der auf dem WLAN übertragenen Daten eingestuft wird, die nötigen Schritte zur Absicherung Ihres Funknetzwerks.

Reinigung und Reparatur

- Das Gerät darf nur durch geschultes Fachpersonal geöffnet werden. Lassen Sie daher Reparaturen am Gerät nur von einer funkwerk-autorisierten Servicestelle durchführen. Wo sich die Servicestelle befindet, erfahren Sie von Ihrem Händler. Durch unbefugtes Öffnen und unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen (z. B. Stromschlag). Unerlaubtes Öffnen der Geräte hat den Garantie- und Haftungsausschluß der Funkwerk Enterprise Communications GmbH zur Folge.

- Das Gerät darf auf keinen Fall naß gereinigt werden. Durch eindringendes Wasser können erhebliche Gefahren für den Benutzer (z. B. Stromschlag) und erhebliche Schäden am Gerät entstehen.
- Niemals Scheuermittel, alkalische Reinigungsmittel, scharfe oder scheuernde Hilfsmittel benutzen.

6.3 Indicaciones generales de seguridad en español

En los siguientes párrafos encontrará indicaciones de seguridad que deberá respetar a la hora de manejar el dispositivo.

Transporte y almacenamiento

- El transporte y almacenamiento del gateway sólo se puede realizar en su embalaje original o en otro embalaje adecuado capaz de protegerlo frente a choques y golpes.
- Observe las indicaciones de transporte y almacenamiento adheridas al embalaje.

Instalación y puesta en funcionamiento

- Antes de la instalación y puesta en funcionamiento del gateway, observe las indicaciones relativas a las condiciones del entorno (consulte datos técnicos y **Guía rápida**).
- Al instalar las conexiones de base externas RDSI tenga en cuenta las normas vigentes en su país. En caso necesario, se deberá recurrir a un técnico debidamente autorizado. Infórmese respecto a las particularidades de los reglamentos nacionales y respete sus bases jurídicas durante la instalación.
- Si la unidad proviene de un entorno frío, al introducirlo en el local de trabajo se puede producir deshielo tanto en su exterior como en su interior. Por ello, antes de ponerlo en funcionamiento espere a que haya adquirido la temperatura ambiente y a que esté totalmente seco. Tenga en cuenta las condiciones medioambientales expuestas en el apartado datos técnicos del manual.
- Asegúrese de que no quede obstaculizado el acceso a la caja de enchufe con puesta a tierra de la instalación. Para desconectar totalmente la unidad de la red es necesario extraer el enchufe de la red.
- Asegúrese de que el valor de los fusibles antepuestos de la conexión de red no sea superior a 16 A.
- Compruebe si la tensión nominal indicada en la placa de características del bloque de alimentación se corresponde con la tensión de red local.

- En el montaje a la pared, asegúrese de que los tornillos están atornillados a la pared de forma segura y pueden soportar el peso de la unidad y del cableado.
- En unidades LAN inalámbricas, asegúrese de que las antenas estén bien atornilladas.
- Al realizar el cableado respete el orden descrito en la **Guía rápida**.
- Antes de poner en funcionamiento el gateway, compruebe si el cableado se ha realizado correctamente, especialmente el cableado RDSI y LAN. La conexión RDSI del gateway no debe estar unida a la conexión Ethernet de su ordenador o hub, y la conexión LAN del gateway no debe estar unida a la conexión RDSI.
- Para el cableado utilice únicamente los cables suministrados o especificados, tal y como se indica en el manual. Si se utilizan otros cables, Funkwerk Enterprise Communications GmbH no se hará responsable en el caso de que se produzcan daños o una merma en el funcionamiento.
- Realice el tendido de cables de tal forma que no supongan ningún peligro (tropiezo) y que no puedan resultar dañados.
- Durante una tormenta, no conecte ni desconecte las líneas de transmisión de datos, ni las toque.

Uso adecuado, funcionamiento

- El gateway está concebido para su uso en oficinas. Como gateway multiprotocolo, establece conexiones WAN en función de la configuración del sistema. Para evitar que se produzcan gastos indeseados, es absolutamente necesario vigilar el producto.
- El gateway cumple las disposiciones de seguridad pertinentes para dispositivos de tecnología de la información destinados a ser utilizados en oficinas. Si tiene dudas relacionadas con la instalación del gateway en el entorno previsto, diríjase a su distribuidor funkwerk o al servicio de atención al cliente de funkwerk.
- El funcionamiento adecuado del sistema conforme a EN 60950 sólo queda garantizado si está montada la tapa de la carcasa (refrigeración, protección contra incendios, eliminación de interferencias de radio).

- La temperatura ambiente no debe ser superior a los 50 °C. Evite que la unidad quede expuesta a la luz solar directa. Cuide de que tenga la suficiente refrigeración.
- Preste atención a que no penetre ningún objeto (p. ej., clips) ni líquido en el interior de la unidad (peligro de descarga eléctrica, cortocircuito).
- Asegúrese de que las ranuras y aberturas de ventilación de la unidad no estén bloqueadas.
- En casos de emergencia (p. ej., carcasa o elemento de mando dañados, penetración de líquido o de algún objeto), interrumpa inmediatamente la alimentación de corriente en el enchufe y avise al servicio técnico.

LAN inalámbrica

- No sitúe el gateway con el componente de radio encendido cerca de gases inflamables o en un entorno con riesgo de explosión (p. ej. taller de barnizado o esmaltado), ya que las ondas de radio que se transmiten podrían provocar una explosión o un incendio.
- El alcance de la comunicación por radio depende de las condiciones medioambientales y del entorno.
- Durante la transmisión de datos mediante una conexión inalámbrica, también es posible que terceras personas no autorizadas reciban datos. Por ello, realice los pasos oportunos para proteger la red inalámbrica, en función del grado de seguridad que requieran los datos transmitidos a través de la WLAN.

Limpieza y reparación

- Sólo personal formado y especializado debe abrir la unidad. Por ello, encargue siempre los trabajos de reparación de la unidad a un servicio técnico autorizado por funkwerk, cuya dirección se la proporcionará su distribuidor. Si se abre de forma no autorizada o las reparaciones no se efectúan como es debido, esto puede suponer riesgos considerables para el usuario (p. ej., descarga eléctrica). Una apertura no autorizada de la unidad supone la pérdida de garantía y la exención de responsabilidad por parte de Funkwerk Enterprise Communications GmbH.
- En ningún caso se debe limpiar la unidad con agua. La penetración de agua puede suponer riesgos considerables para el usuario (p. ej., descarga eléctrica) así como daños considerables para la unidad.

- No utilice nunca medios abrasivos, productos de limpieza alcalinos ni agentes auxiliares agresivos o abrasivos.

6.4 Consignes générales de sécurité en français

Les paragraphes suivants énoncent les consignes de sécurité à observer lors de l'utilisation de votre appareil.

Transport et stockage

- Transportez et stockez votre passerelle uniquement dans son emballage d'origine ou dans un emballage anti-chocs adapté.
- Observez les instructions de transport et de stockage figurant sur l'emballage.

Installation et mise en service

- Lisez les informations relatives aux conditions environnementales avant d'installer et de mettre en service la passerelle (voir les caractéristiques techniques et le **Bref mode d'emploi**).
- Observez les conditions générales en vigueur dans votre pays lors de l'installation d'accès de base externes. Le cas échéant, faites appel à un technicien agrée. Renseignez-vous sur les spécificités de la législation de votre pays et observez la législation en vigueur lors de l'installation.
- Lorsque l'appareil est transféré d'un environnement froid vers son lieu d'exploitation, de la condensation peut se former à l'extérieur et à l'intérieur de l'appareil. Attendez que l'appareil soit à la température ambiante et sec avant de le mettre en service. Respectez les conditions environnementales indiquées dans le chapitre caractéristiques techniques.
- Vérifiez que la prise de contact de protection de l'installation est accessible. Retirez la fiche secteur pour une mise hors tension complète.
- Vérifiez que les fusibles en amont de la connexion au secteur ne dépassent pas 16 A.
- Vérifiez que la tension nominale indiquée sur la plaque signalétique de l'alimentation correspond à la tension secteur locale.
- En cas de montage mural, vérifiez que les vis sont bien fixées au mur et qu'elles sont capables de supporter le poids et le câblage de l'appareil.
- Veillez à ce que les antennes des appareils de réseau local sans fil soient bien vissées.

- Respectez l'ordre de câblage indiqué dans le **Bref mode d'emploi**.
- Vérifiez l'acheminement des câbles (notamment les câbles RNIS et du réseau local) avant de mettre en service la passerelle. La connexion RNIS de votre passerelle ne doit pas être reliée à la connexion Ethernet de l'ordinateur ou du concentrateur et la connexion au réseau local de la passerelle ne doit pas être reliée à la connexion RNIS.
- Utilisez uniquement les câbles fournis ou spécifiés, comme cela est indiqué dans le manuel. Si vous utilisez d'autres câbles, Funkwerk Enterprise Communications GmbH ne sera pas responsable des éventuels dommages ou dysfonctionnements.
- Posez les câbles de manière à ce qu'ils ne représentent aucun danger (trébuchement) et ne risquent pas d'être endommagés.
- Pendant un orage, ne raccordez pas les câbles de transmission des données, ne les débranchez pas et ne les touchez pas.

Utilisation conforme, fonctionnement

- Votre passerelle convient à une utilisation dans un bureau. En tant que passerelle multiprotocole, la passerelle établit des connexions WAN (réseau étendu) en fonction de la configuration du système. Pour éviter des frais inutiles, surveillez le produit.
- La passerelle est conforme aux normes de sécurité en vigueur pour les dispositifs des technologies de l'information pour une utilisation dans un bureau. Si vous souhaitez savoir si vous pouvez installer la passerelle dans votre environnement, contactez votre revendeur funkwerk ou le service client funkwerk.
- L'utilisation conforme du système selon EN 60950 est uniquement garantie lorsque le couvercle du boîtier est monté (refroidissement, protection incendie, antiparasitage).
- La température ambiante ne doit pas dépasser 50 °C. Evitez l'exposition directe aux rayons du soleil. Veillez à ce que le refroidissement soit suffisant.
- Vérifiez qu'aucun objet (par ex. trombones) ou liquide ne pénètre dans l'appareil (choc électrique, court-circuit).
- Vérifiez que les fentes et orifices de ventilation de l'appareil ne sont pas bloqués.

- En cas d'urgence (par ex. boîtier ou élément de commande défectueux, pénétration de liquide ou de corps étrangers), coupez l'alimentation de la prise et contactez la maintenance.

Réseau local sans fil

- Ne pas positionner la passerelle avec des composants sans fil actifs à proximité de gaz inflammables ou dans un environnement présentant un risque d'explosion (par ex. atelier de peinture) car les ondes radio transmises peuvent déclencher une explosion ou un incendie.
- La portée de la liaison radio dépend des conditions environnementales et ambiantes.
- En cas de transmission de données via une connexion sans fil, il se peut qu'un tiers non autorisé reçoive les données. Prenez des mesures de sécurité adéquates en fonction de la sensibilité des données échangées sur le réseau local sans fil.

Nettoyage et entretien

- L'appareil ne doit être ouvert que par le personnel habilité. Faites réparer l'appareil uniquement par un centre de maintenance agrée de funkwerk. Votre revendeur vous indiquera le centre de maintenance le plus proche. L'ouverture non autorisée et les réparations non conformes peuvent entraîner la mise en danger de l'utilisateur (par ex. choc électrique). L'ouverture non autorisée de l'appareil a pour conséquence l'annulation de la garantie et la non responsabilité de Funkwerk Enterprise Communications GmbH.
- Ne pas nettoyer l'appareil avec un chiffon humide. La pénétration d'eau dans l'appareil peut entraîner la mise en danger de l'utilisateur (par ex. choc électrique) ou endommager l'appareil.
- Ne pas utiliser d'abrasif, de nettoyant alcalin, d'accessoire coupant ou abrasif.

6.5 Indicazioni generali di sicurezza in italiano

Nei paragrafi che seguono sono riportate le indicazioni di sicurezza che devono essere sempre rispettate nell'uso dell'apparecchio.

Trasporto e magazzinaggio

- Trasportare e mettere a magazzino il router soltanto nell'imballaggio originale o in un altro imballaggio che lo protegga da urti e colpi.
- Rispettare le indicazioni per il trasporto e il magazzinaggio riportate sull'imballaggio.

Installazione e messa in funzione

- Prima di installare e mettere in funzione il router, verificare le indicazioni relative alle condizioni ambientali (cfr. dati tecnici del manuale e la **Guida Rapida**).
- Quando si installano interfacce base ISDN esterne, rispettare le norme nazionali in vigore. Può essere necessario l'intervento di un tecnico che disponga dell'autorizzazione richiesta. Informarsi sulle particolarità delle norme nazionali e rispettare i requisiti legali per l'installazione.
- Se l'apparecchio viene trasferito nel locale di esercizio da un ambiente freddo, è possibile che si formi condensa sia al suo esterno sia all'interno. Prima di mettere in funzione l'apparecchio, attendere che esso si sia portato a temperatura ambiente e che sia assolutamente asciutto. Rispettare le indicazioni relative alle condizioni ambientali riportate nel capitolo dati tecnici del manuale.
- Accertare che la presa munita di contatto di terra dell'impianto sia liberamente accessibile. Per staccare completamente l'apparecchio dalla rete di alimentazione è necessario estrarre la spina.
- Verifiare che il valore dei fusibili a monte del collegamento di rete non superi 16 A.
- Verificare che la tensione nominale specificata sulla targhetta dell'alimentatore coincida con la tensione di rete locale.
- In caso di montaggio a parete, accertare che le viti siano saldamente avvitate alla parete e che siano in grado di sopportare il peso dell'apparecchio e del cablaggio.

- In caso di apparecchi LAN con collegamento radio, verificare che le antenne siano saldamente avvitate.
- Per il cablaggio rispettare la sequenza descritta nella **Guida Rapida**.
- Prima di mettere in funzione il router, verificare se il cablaggio – in particolare il cablaggio ISDN e LAN – è stato eseguito correttamente. L'attacco ISDN del router non deve essere collegato con l'attacco Ethernet del vostro computer o hub, l'attacco LAN del router non deve essere collegato con il vostro attacco ISDN.
- Per il cablaggio utilizzare soltanto i cavi forniti o comunque quelli specificati, come descritti nel manuale. In caso di impiego di cavi diversi, Funkwerk Enterprise Communications GmbH non risponde dei danni o della riduzione di funzionalità risultanti.
- Posare i cavi in modo che non siano potenzialmente pericolosi (inciampo) e che non possano essere danneggiati.
- Durante un temporale, non collegare o disconnettere o toccare i cavi di trasmissione dati.

Uso previsto, esercizio

- Il router è concepito per essere impiegato in ambiente di ufficio. In qualità di router multiprotocollo, il router realizza i collegamenti WAN in rapporto alla configurazione del sistema. Per evitare canoni imprevisti, il prodotto dovrebbe essere sempre tenuto sotto controllo.
- Il router è conforme alle norme di sicurezza applicabili per apparecchiature informatiche in ambiente di ufficio. Se si hanno dubbi sulla possibilità di installare il router nell'ambiente previsto, rivolgersi al rivenditore funkwerk o al servizio di assistenza funkwerk.
- Il corretto funzionamento del sistema secondo EN 60950 è garantito soltanto se è installato il coperchio dell'involucro (raffreddamento, protezione antincendio, schermatura contro radiodisturbi).
- La temperatura ambiente non dovrebbe superare 50 °C. Evitare l'esposizione diretta ai raggi solari. Provvedere a un sufficiente raffreddamento.
- Evitare che oggetti estranei (p. es. fermagli) o liquidi possano penetrare nell'apparecchio (pericolo di scosse elettriche, cortocircuito).

- Accertare che le fessure e le aperture di ventilazione dell'apparecchio non siano bloccate.
- In caso di emergenza (p. es. danni all'involucro o all'elemento di comando, penetrazione di liquidi o di oggetti estranei) staccare immediatamente la spina di alimentazione e informare il servizio di assistenza.

LAN con collegamento radio

- Non portare il router con componenti radio inseriti in vicinanza di gas infiammabili o in un ambienti a rischio di esplosione (p. es. un officina di verniciatura), poiché le onde radio trasmesse possono provocare un'esplosione o un incendio.
- La portata utile del collegamento radio dipende dalle condizioni ambientali.
- I dati trasmessi con collegamento senza fili possono essere ricevuti anche da terzi non autorizzati. A seconda del livello di criticità dei dati trasmessi tramite WLAN, attivare i provvedimenti necessari per mettere in sicurezza la rete radio.

Pulizia e riparazione

- L'apparecchio deve essere aperto soltanto da personale specializzato e addestrato. Pertanto affidare le riparazioni soltanto ad un centro di assistenza funkwerk autorizzato. Il rivenditore può fornire informazioni sugli indirizzi di tali centri di assistenza. L'apertura da parte di personale non autorizzato e riparazioni non corrette possono comportare gravi pericoli per l'utilizzatore (p. es. scossa elettrica). L'apertura non autorizzata degli apparecchi comporta l'annullamento della garanzia e della responsabilità della Funkwerk Enterprise Communications GmbH.
- In nessun caso si deve pulire l'apparecchio con acqua. L'infiltrazione di acqua può comportare gravi pericoli per l'utilizzatore (p. es. scossa elettrica) e notevoli danni all'apparecchio.
- In nessun caso utilizzare detergenti alcalini o attrezzi affilati o abrasivi.

6.6 Ogólne instrukcje bezpieczeństwa w języku polskim

W kolejnych podrozdziałach zawarte są instrukcje bezpieczeństwa, których należy bezwzględnie przestrzegać podczas obsługi urządzenia.

Transport i przechowywanie

- Bramę należy transportować i przechowywać jedynie w oryginalnym opakowaniu lub innym odpowiednim opakowaniu, zapewniającym ochronę przed uszkodzeniami mechanicznymi.
- Należy przestrzegać wskazówek dotyczących transportu i przechowywania, znajdujących się na opakowaniu.

Ustawianie i uruchamianie

- Przed ustawieniem i rozpoczęciem eksploatacji bramy należy zapoznać się ze wskazówkami dotyczącymi warunków otoczenia (por. rozdziały dane techniczne i krótkie wprowadzenie).
- Podczas instalacji zewnętrznych złączy bazowych ISDN należy uwzględnić uwarunkowania techniczne obowiązujące w danym kraju. W razie potrzeby należy skorzystać z pomocy specjalisty posiadającego odpowiedni certyfikat. Należy zapoznać się z informacjami na temat szczególnych rozporządzeń obowiązujących w danym kraju oraz przestrzegać przepisów prawnych podczas instalacji.
- W razie przeniesienia urządzenia z zimnego otoczenia do pomieszczenia eksploatacyjnego może dojść do powstania skroplin zarówno wewnątrz, jak i na zewnątrz urządzenia. Przed uruchomieniem należy odczekać, aż temperatura urządzenia zrówna się z temperaturą nowego otoczenia oraz urządzenie będzie całkowicie suche. Należy także przestrzegać zaleceń dotyczących warunków środowiskowych zawartych w rozdziale dane techniczne.
- Podczas instalacji należy zapewnić swobodny dostęp do gniazda wtykowego z zestykiem ochronnym. Aby całkowicie odłączyć zasilanie, należy wyciągnąć wtyczkę sieciową z gniazda.
- Wartość bezpieczników umieszczonych przed przyłączeniem sieciowym nie powinna przekraczać 16 A.

- Należy sprawdzić, czy napięcie nominalne podane na tabliczce znamionowej zasilacza sieciowego jest zgodne z lokalnym napięciem sieciowym.
- W razie montażu ściennego należy upewnić się, że śruby zostały prawidłowo osadzone w ścianie i są w stanie udźwignąć ciężar urządzenia wraz z okablowaniem.
- Należy zwrócić uwagę, aby anteny radiowych urządzeń sieci LAN zostały mocno przykręcone.
- Podczas instalacji okablowania należy przestrzegać kolejności podanej w rozdziale krótkie wprowadzenie.
- Przed uruchomieniem bramy należy sprawdzić, czy okablowanie (zwłaszcza okablowanie ISDN i LAN) zostało prawidłowo poprowadzone. Złącze ISDN bramy nie może być połączone ze złączem Ethernet komputera lub hubem; złącze LAN bramy nie może być połączone ze złączem ISDN.
- Okablowanie należy wykonać wyłącznie z dostarczonych lub zgodnych ze specyfikacją kabli, zgodnie z opisem w podręczniku. W przypadku użycia innych kabli firma Funkwerk Enterprise Communications GmbH nie ponosi odpowiedzialności za wystąpienie szkód lub ograniczenie funkcjonalności.
- Przewody należy poprowadzić w taki sposób, aby nie stwarzały one zagrożenia (niebezpieczeństwo potknięcia) i nie uległy uszkodzeniu.
- Podczas burzy nie wolno przyłączać, odłączać ani dotykać przewodów transmisji danych.

Użytkowanie zgodne z przeznaczeniem oraz eksploatacja

- Brama jest przeznaczona do użytku biurowego. Jako brama wieloprotokołowa urządzenie to realizuje połączenia w sieci WAN w zależności od konfiguracji systemowej. Aby uniknąć niezamierzonych opłat, urządzenie należy koniecznie nadzorować.
- Brama jest zgodna z właściwymi przepisami bezpieczeństwa dotyczącymi urządzeń informatycznych przeznaczonych do użytku biurowego. W przypadku pytań dotyczących użytkowania bramy w danym środowisku należy skontaktować się z punktem sprzedaży produktów firmy funkwerk lub biurem obsługi klienta firmy funkwerk.
- Zgodnie z normą EN 60950, praca systemu zgodna z przeznaczeniem jest zagwarantowana jedynie przy zamontowanej pokrywie obudowy (z uwagi

na chłodzenie, ochronę przeciwpożarową oraz eliminację zakłóceń radiowych).

- Temperatura otoczenia nie powinna przekraczać 50 °C. Należy unikać bezpośredniego działania promieni słonecznych. Należy zapewnić wystarczające chłodzenie.
- Należy uważać, aby do wnętrza urządzenia nie dostały się żadne przedmioty (np. spinacze biurowe) lub płyny (niebezpieczeństwo porażenia prądem, zwarcie).
- Należy upewnić się, że szczeliny i otwory wentylacyjne urządzenia nie zostały zablokowane.
- W przypadku sytuacji awaryjnej (np. uszkodzenie obudowy lub podzespołu, przedostanie się cieczy lub ciała obcego do środka urządzenia) należy natychmiast odłączyć zasilanie przy gnieździe zasilania i skontaktować się z serwisem.

Radiowa sieć LAN

- Nie wolno przenosić bramy z włączonym podzespołem radiowym w miejsce występowania łatwopalnych gazów lub w otoczenie zagrożone wybuchem (np. lakiernia), ponieważ transmitowane fale radiowe mogą wywołać pożar lub wybuch.
- Zasięg połączenia radiowego zależy od warunków środowiskowych i otoczenia.
- Podczas transferu danych poprzez połączenie bezprzewodowe istnieje możliwość odbioru danych przez nieuprawnione osoby trzecie. Dlatego należy podjąć właściwe kroki mające na celu zabezpieczenie sieci radiowej, odpowiednio do przyjętego stopnia ważności danych przesyłanych z wykorzystaniem sieci WLAN.

Czyszczenie i naprawa

- Tylko wykwalifikowany personel może otwierać urządzenie. Z tego powodu przeprowadzenie naprawy urządzenia należy zlecać tylko punktom serwisowym autoryzowanym przez firmę funkwerk. Adresy punktów serwisowych można otrzymać w punktach sprzedaży. Otwieranie urządzenia przez osoby nieupoważnione i niewłaściwe przeprowadzone naprawy mogą stwarzać poważne zagrożenia dla użytkownika (np. porażenie prądem). Otwarcie urządzenia przez osoby nieupoważnione powoduje unieważnien-

ie gwarancji i wyłączenie odpowiedzialności firmy Funkwerk Enterprise Communications GmbH.

- Czyszczenie urządzenia na mokro jest absolutnie zabronione. Przedostająca się do wnętrza woda może stworzyć poważne niebezpieczeństwo dla użytkownika (np. porażenie prądem) oraz uszkodzić urządzenie.
- Nie wolno stosować środków do szorowania, alkalicznych środków czyszczących oraz środków żrących lub ściernych.

6.7 Considerações genéricas em matéria de segurança, em português

Nos parágrafos que se seguem, encontra considerações em matéria de segurança que terá de respeitar estritamente ao lidar com o aparelho.

Transporte e armazenamento

- Transporte e armazene o Gateway apenas na embalagem original ou noutra embalagem adequada para o efeito que o proteja contra embates fortes e pancadas.
- Tenha em atenção as indicações de transporte e armazenamento indicadas na embalagem.

Instalação e colocação em funcionamento

- Antes de proceder à instalação e colocação em funcionamento do Gateway, siga as indicações relativas às condições ambientais (cf. dados técnicos e **Instruções Breves de Utilização**).
- Aquando da instalação de conexões externas de base RDIS, respeite as respectivas condições básicas em vigor no seu país. Se necessário, a instalação deverá ser efectuada por um técnico que disponha de licença para tal. Informe-se acerca das particularidades dos regulamentos nacionais e respeite o respectivo fundamento legal aquando da instalação.
- Quando o aparelho é deslocado de um local frio para o local de funcionamento, poderá haver formação de condensação tanto no exterior como no interior do aparelho. Aguarde até que o aparelho se encontre à temperatura ambiente e completamente seco antes de o colocar em funcionamento. Tenha em atenção as indicações relativas às condições ambientais no capítulo do manual dados técnicos.
- Certifique-se de que a tomada de contacto de segurança da instalação está acessível. Para desligar completamente a corrente do aparelho, retire a ficha de rede.
- Certifique-se de que o valor da protecção da ligação à rede não ultrapassa 16 A.
- Verifique se a tensão nominal indicada na placa de características do fornecimento de energia está de acordo com a tensão de rede local.

- Em caso de montagem na parede, certifique-se de que os parafusos são fixados de modo seguro à parede e que conseguem aguentar o peso do aparelho e da cablagem.
- Em caso de aparelhos LAN sem fios, certifique-se de que a antena está bem fixa.
- Ao proceder à cablagem, respeite a sequência tal como está descrita nas **Instruções Breves de Utilização**.
- Antes de colocar o Gateway em funcionamento, verifique se a cablagem – em especial a cablagem RDIS e LAN – foi efectuada correctamente. A ligação RDIS do Gateway não deve ser conectada à ligação Ethernet do seu computador ou do hub; a ligação LAN do Gateway não deve ser conectada à ligação RDIS.
- Para a cablagem, utilize unicamente o cabo anexado ou especificado, conforme descrito no manual. Se utilizar outro cabo, a Funkwerk Enterprise Communications GmbH não se responsabiliza por danos daí decorrentes ou por limitações de funcionamento.
- Instale os cabos de maneira a não constituírem uma fonte de perigo (perigo de tropeçar), nem se danificarem.
- Em caso de trovoada, não ligue, nem retire ou toque nos cabos de transmissão de dados.

Utilização conforme as especificações, funcionamento

- O Gateway destina-se à utilização em escritórios. Como Gateway de protocolos múltiplos, o Gateway constrói ligações WAN de acordo com a configuração do sistema. Para evitar custos indesejados, deverá controlar incondicionalmente o produto.
- O Gateway corresponde às normas de segurança habituais relativas a dispositivos de informática para utilização em escritórios. Caso tenha dúvidas se o Gateway pode ser instalado no local previsto, consulte o seu agente funkwerk ou o Suporte Técnico da funkwerk.
- O funcionamento conforme as especificações EN 60950 só é garantido com a tampa da caixa montada (refrigeração, protecção contra incêndios, supressão de ruído)

- A temperatura ambiente não deve exceder os 50 °C. Evite expor o aparelho à luz solar directa. Verifique se a refrigeração é suficiente.
- Tenha o cuidado de não deixar entrar objectos (p.ex. clipes) ou líquidos para o interior do aparelho (choque eléctrico, curto-circuito).
- Certifique-se de que as ranhuras e aberturas de ventilação do aparelho não estão bloqueadas.
- Em caso de emergência (p.ex. caixa ou elemento de comando danificado, entrada de líquido ou de corpos estranhos), interrompa imediatamente a alimentação de corrente e recorra ao serviço de assistência técnica..

LAN sem fios

- Não aproxime o Gateway em transmissão de gases inflamáveis nem o coloque num local onde haja risco de explosão (por exemplo, oficina de pintura), pois as ondas de rádio transmitidas podem originar uma explosão ou incêndio.
- O alcance da transmissão depende das condições climatéricas e das condições do local.
- Em caso de tráfego de dados através de uma ligação sem fios é também possível que terceiros não autorizadas recebam dados. Por conseguinte, tome os passos necessários para proteger a rede sem fios consoante a classificação de segurança dos dados transmitidas via WLAN.

Limpeza e reparação

- O aparelho só pode ser aberto por pessoal especializado. Por conseguinte, deixe as reparações do aparelho exclusivamente a cargo dos serviços de assistência técnica funkwerk autorizados. Informe-se junto do seu agente para saber onde encontrar um ponto de assistência técnica. Uma abertura não autorizada e reparações inadequadas podem representar riscos graves para o utilizador (p.ex., choque eléctrico). Uma abertura não autorizada do aparelho tem como consequência a perda da garantia e da responsabilidade da Funkwerk Enterprise Communications GmbH.
- O aparelho nunca deverá ser limpo a húmido. A infiltração de água pode constituir perigo para o utilizador (p.ex. choque eléctrico) e danos graves no aparelho.
- Nunca deverão ser utilizados abrasivos, produtos de limpeza alcalinos, objectos afiados ou que risquem.

R&TTE Compliance

This R&TTE compliance leaflet contains information for ... products of the brands ... and their compliance with the EC Directive 1999/5/EC (R&TTE Directive) relevant to the European Union. This document is valid for all single band products (2,4 GHz, IEEE802.11b/g) and for all dual band products (2,4 GHz, IEEE802.11b/g and 5 GHz, IEEE802.11a/h).

EC Declaration of Conformity

Bulgaria (BG) България	Настоящият уред отговаря на основните изисквания и на по-нататъшните съответни параметри на директива 1999/5/EC
Czech (CS) Česky	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními směrnice 1999/5/ES
Danish (DA) Dansk	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Dutch (NL) Nederlands	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EG
Estonian (ET) Eesti	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English (EN)	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC
German (DE) Deutsch	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EG
Greek (EL) Ελληνική	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/ΕΚ
Finnish (FI) Suomi	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.

French (FR) Français	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/CE
Hungarian (HU) Magyar	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Icelandic (IS) Íslenska	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EB
Italian (IT) Italiano	Questo apparato è conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE
Latvian (LV) Latviski	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian (LT) Lietuvių	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Maltese (MT) Malti	Dan l-apparat huwa konformi mal-htigiet essenzjali u l-provedimenti l-ohra rilevanti tad-Direttiva 1999/5/KE
Norwegian (NO) Norsk	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv.1999/5/EC
Polish (PL) Polski	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/WE
Portuguese (PT) Português	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/CE
Romania (RO) Română	Acest echipament este in conformitate cu cerintele esentiale si cu alte prevederi relevante ale Directivei 1999/5/EC.
Spain (ES) Español	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE
Slovenian (SL) Slovensko	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/ES

Slovak (SK) Slovensky	Toto zariadenie je v súlade so základnými požiadavkami a ostatnými príslušnými ustanoveniami smernice 1999/5/ES
Swedish (SV) Svenska	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i direktiv 1999/5/EG

Note

The EC declaration of conformity can be found at ....

Applied standards for the EC declaration of conformity:

Radio Spectrum:

- Single band and dual band products:
  - EN 300 328 for sub-band a) 2400 - 2483.5 MHz
  - Dual band products only:
    EN 301 893 for sub-bands b) 5150 - 5250 MHz, c) 5250 - 5350 MHz, d) 5470 - 5725 MHz

Safety:

- Single band and dual band products:
  - EN 60950-1
  - EN 50371

Electromagnetic Compatibility (EMC):

- Single band and dual band products:
  - EN 301 489-1
  - EN 301 489-17

CE Marking

This Product is intended to be operated in the following countries: AT, BE, BG, CY, CZ, DK, EE, FI ,FR ,DE, GR, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, RO, SK, SI, ES, SE, GB, NO, CH, LI.

The following conformity mark is added to the WLAN product in accordance to annex VII of 1999/5/EC:

For some products a Notified Body was consulted. In this case its number is noted between CE and the alert symbol (!). You can find detailed product specific information at ....

National Restrictions and Requirements for Authorization

In accordance to article 6 (3) of 1999/5/EC we herewith inform you about the national restrictions and requirements for authorization in the following countries (see table below). The requirements for any country may evolve. ... recommends that you check with local authorities for the latest status of their national regulations for both 2.4 and 5 GHz wireless LANs.

Frequency Band	Restrict-ions	RF - Radiated Power	Comments
2400 - 2454 MHz	None	100 mW e.i.r.p.	Class 1
2400 - 2483.5 MHz	None	10 mW e.i.r.p.	Class 1
2454 - 2483.5 MHz	Yes	100 mW e.i.r.p.	Class 2
5150 - 5250 MHz	Yes		Class 2
5250 - 5350 MHz	Yes		Class 2
5470 - 5725 MHz	Yes		Class 2

Note

The 5-GHz equipment meets the Dynamic Frequency Selection (DFS) requirements applicable to client cards (slaves) as defined in ETSI EN 301 893.

In order to meet the Transmit Power Control (TPC) requirement, the equipment has different user-selectable power levels from which the maximum power level is 3 dB below the applicable limit.

The following sections identify countries having additional requirements for authorization or restrictions other than those listed in the table above (indicated by "Yes" in the column "Restrictions").

Note

Please note that this table might not be up to date as you read it. Despite careful research on the subject, there may be regulations in countries which are not mentioned here. If you are uncertain about your national regulations, please contact your national regulatory authority!

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark er frekvensbåndene 5150 - 5350 MHz også tilladt til udendørs brug.

France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used in other parts of the 2,4 GHz band. Check http://www.arcep.fr/ for more details.

Pour 2,4 GHz, la puissance de sortie est limitée à 10 mW PIRE lorsque le produit est utilisé à l'extérieur dans la bande 2 454 - 2 483,5 MHz. Il n'y a pas de limitation dans le cas d'une utilisation dans les autres parties de la bande 2,4 GHz. Pour obtenir de plus amples informations, consultez le site http://www.arcep.fr/.

Italy

This product meets the National Radio Interface specifications and the requirements in the National Frequency Allocation Table for Italy. Operating wireless equipment requires a "general authorization" unless it is operated within the boundaries of the owner's property. Please check with http://www.comunicazioni.it/it for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.comunicazioni.it/it per maggiori dettagli.

Latvia

The outdoor usage of the 2.4-GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

Ārēja 2.4-GHz grupas lietošana pieprasa Electronic Communications Office (Elektronisko sakaru biroja) atļauju. Sīkākām detaļām izvēlieties, lūdzu, http://www.esd.lv.

Antennas

This Product is to be operated with the antennas supplied with the equipment. Other antennas may be used, but then the operator is responsible for fulfilling the local regulations. In general this means that, when high gain antennas are used, the output power must be decreased accordingly.

Operating Frequency

The operating frequency is determined by the access point to which the client is associated. The operating frequency of the client cannot be set manually. It is important that the Access Point is correctly configured to meet the local regulations. Please select your country in the country settings of the Access Point.

Changing Output Power

Please refer to the manual of your device in order to manually reduce the output power.

Obtaining Documents from www.funkwerk-ec.com

Please browse to http://.... For further questions you can also contact

...